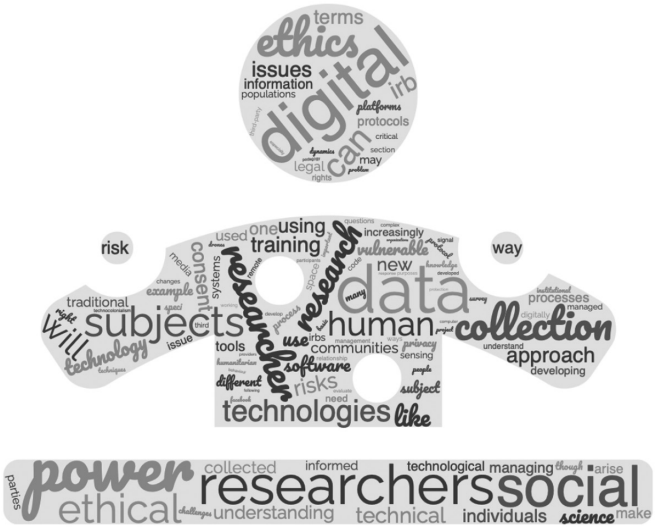
Suggested Citation:
Martin-Shields, Charles & Ziad al Achkar. 2023. "Human Subjects, Digital Protocols: The Future of Institutional Review Boards (IRBs) and Digital Research in Vulnerable Communities," in Personal Data Collection Risks in a Post-Vaccine World. Colette Mazucelli, James Felton Keith, and C. Ann Hollifield eds. New York: Anthem Press. pp. 25-43.

Chapter 2

# HUMAN SUBJECTS, DIGITAL PROTOCOLS: THE FUTURE OF INSTITUTIONAL REVIEW BOARDS (IRBS) AND DIGITAL RESEARCH IN VULNERABLE COMMUNITIES

Charles Martin-Shields and Ziad Al Achkar




## Introduction: New Pedagogy for Digital Human Subjects Research

Ethics in human subjects research, whether in medical or social sciences, has been a key topic in researchers' training for decades in the United States and United Kingdom (UK). In the United States, the history of IRBs in evaluating and overseeing the conduct of ethical human subjects

research has its roots in legislation. The 1974 National Research Act was signed into law after a series of congressional hearings on human subjects research and gained greater momentum in response to the Tuskegee syphilis study (Chadwick, 1997). In the UK the processes have been more decentralised with research ethics committees distributed across research sectors and universities, but since the early 2000s there have been greater efforts to develop national standards for both biomedical and social science human subjects research in the UK. While these standards are world leading, and many developing countries are adopting their own human subjects research frameworks based on them, the advent of widespread digital data collection presents new challenges for researchers and educators to address in ethics and research protocol pedagogy. This is especially true when research is being done in and with vulnerable subjects in developing countries.

How we address this question has implications for general society as well as academic research. Complex power relations emerge in this space between a university's IRB's conception of ethical human subjects research and a technology's terms of use, including those between the researcher and participant, and the researcher and software company. As the nature of research adapts and incorporates technological changes, the IRB will increasingly be the facility that mediates the power of different actors in a digital human subjects research process to make sure research participants are protected.

Increasingly, the interface between digital research and peoples' daily online behaviour is blurring. When we, for example, use Twitter, it is possible that this mundane activity is producing data that can be used by a researcher. This type of relationship would be governed by a platform's terms of use, to which a researcher who uses Twitter or social media data must conform. But there is a great distance between a technology platform's terms of use, which fundamentally protects the business interests of the software firm, and the standards for doing human subjects research that the researcher is expected to uphold. Within this space are elements of power. There is the software firm where data is provided and housed, and for which data is a profit-making medium; the researcher, who is seeking to undertake research using digital data and has a wider scope of knowledge than the research participants about what this work entails; and the university itself, for which ethical human subjects research is tightly interwoven with managing the risk of culpability in the case that harm comes to a research subject. Between these actors and the research subject is the IRB, which must assess and mediate the power of the different actors to protect both the research subject and the firm, researcher and university from each other. So how does

Personal Data Collection Risks in a Post-Vaccine World.indb 26 14-10-2022 11:10:24

an IRB, traditionally an analogue construct, moderate different aspects of power in the digital era?

The first issue to address is understanding the unique risks that digital systems bring to human subjects research. Digital survey tools like KoBo Toolbox have been used for a number of years to do traditional survey research, but these are different than digital platforms that involve third-party software and cloud data storage. Doing a survey is ethically different than using social media platforms for experiments or remote sensing/passive data collection in vulnerable communities. The passive/remote sensing tools bring up a basic issue in research protocols, the main area where the research subject has power: informed consent. Because social media and remote sensing systems derive their utility by being autonomous and may remain in a fixed location gathering data many times over, the process of defining an informed consent process is made more complex. The second issue, the 'permanence' of digital data, is less tangible and demands a wider range of risk analysis on the part of the researcher. Unlike paper, a digital record can be replicated and shared widely in a way that defies deletion. What does this mean for research protocols and ethics in vulnerable communities, especially those who may be at risk for years after the research takes place? The first section of this chapter will address these issues in relation to standard approaches to human subjects research protocol training and lead into the second section that grapples with the current gaps in ethics and protocol training when using digital tools.

The second section of the chapter goes into greater detail on what is covered in traditional ethics and protocol training, with a specific focus on social sciences. It will unpack the issues that arise with informed consent, managing power relations and other sociological components that are critical to ethical human subjects research. After doing this, the section will explore how this training falls short in preparing researchers to use digital tools in their research, exploring the skills and training gaps that would need to be filled to fully prepare researchers to work digitally with vulnerable communities.

In many ways what makes digitally based research unique is that the relationships and power dynamics between the researcher and subject are interjected by the digital medium. Inherent to this medium are user agreements, issues with data ownership and the role that third-party software providers play in supporting or undermining best practices in ethics and research protocols. Thus, the purpose is not to develop a tool-to-match process by which we identify specific rights, requirements or risks with each specific technology that would apply to each scenario, but rather develop a holistic approach that

Personal Data Collection Risks in a Post-Vaccine World.indb 27 14-10-2022 11:10:24

guarantees rights of individuals and groups whose data is collected that would transcend a specific technological innovation. The role of digitally literate and equipped IRB would be to therefore evaluate how the proposed project or technological tool used guarantees the rights of individuals, reduces risks and safeguards against harm.

The chapter closes with final conclusions on the future of digital research, including both the opportunities and risks that come with using new digital tools to do human subjects research and what these mean for society more broadly.

## What Makes Digital Research Unique(ly Risky)?

The current state of research protocol and ethics training covers a wide range of ethical and risk management issues. Topics like informed consent, data protection, and privacy and anonymity are well-covered ground in most human subjects research and ethics courses. The problem is that digitally intermediated research, using social media platforms and proprietary data collection systems, introduces a whole suite of risks that go beyond legal processes like informed consent or procedural issues like securing respondent data on a host computer. This section will cover three ways in which digital systems can lead to breakdowns in different aspects of human subjects research protocols: the first is the automatic nature of digital systems, the second is the 'permanence' of digital data and the third is the speed of technological change outpacing regulatory or oversight capacity. When we overlay these three aspects of digital data collection across the standard rules and regulations that go into ethics protocols, we can begin to see how digital platforms for data collection present new, unique risks for doing human subjects research in an ethical way.

The first issue, passive and automatic data collection, brings up specific problems of informed consent. For example, if a researcher is using drones to collect imaging data of a village or populated area how do they make sure that each round of data collection meets consent rules? WeRobotics,[1] a social impact firm that focuses on the effective and inclusive use of drones and robotics in humanitarianism and development, provides a framework that could be applied in an IRB framework. They recommend limiting flight time and data collection to only that which is necessary, coordinating with communities and sharing information on flight activities, and knowing/respecting local regulations and political sensitivities when flying drones. This may be easier to manage if we are the pilots and are flying the drones at a specific time on specific

1 https://werobotics.org/

Personal Data Collection Risks in a Post-Vaccine World.indb 28 14-10-2022 11:10:24

days for a set number of flights; in such a case we would write the entire flight schedule into the informed consent form, have meetings with residents and show them footage after the first flight, and generally make sure that the research subjects are aware of the entire process. But what if we are doing an experiment that relies on the drones to fly autonomously in response to certain environmental conditions? We may not know how many times they will fly, the image quality, who will be out of their house during flights and the impact that flights during sleeping hours may have. Again, this can be written into an informed consent document and routine meetings with communities can help identify tensions, but the randomness of the flights can add complexity to consent. Following the WeRobotics approach, we have to go beyond just flight management – a researcher needs to get training on flying drones and risk management that is specific to drone operations, create contingency plans for accidents and make their data collection strategy as publicly known. If an IRB is making power central to an ethics process, training and planning are precisely the kind things that a researcher would need to do to manage and direct their power vis-à-vis the communities with which they are doing research.

At the sharpest end of consent issues are remote sensing tools. For example, a researcher may want to do an experiment that tracks locals' mobility. This kind of data collection is done by cities all the time, and urban planning researchers have used passive systems to track urban mobility for years (e.g. Bhatta et al., 2010). In these cases, though, these were not overtly vulnerable populations, and the research subjects were using public infrastructure – a sign explaining what data are being collected and where to find more information could be sufficient, depending on local ordinances. But what if one is working in a vulnerable community, for example, one affected by violent conflict? The use of drones and sensing systems has led to ethical problems in practice settings such as peacekeeping operations (Andrews, 2017; Lidén and Sandvik, 2016).

Using passive sensors to register movement and sounds for research purposes creates serious informed consent problems. From a methodological perspective, we may want to know how people move in the natural rhythm of their day, explaining that there are unseen sensors in the environment could adversely affect their normal behaviour. There is another problem, too: What counts as a single round of data collection? Normally any time someone gathers data, they have to ask permission. This is impossible if sensors are picking up new data hundreds or thousands of times a day. Finally, what happens when someone refuses to consent? The sensor is operating in an open space, and the researcher may not know if the anonymised data the sensor picks up is from the person who did not consent. One could just shrug and run the research, but this runs directly

Personal Data Collection Risks in a Post-Vaccine World.indb 29 14-10-2022 11:10:24

contrary to standard ethical practice. This creates a large problem for researchers and raises important questions of what the protocol ought to be in those cases. Should the dataset be completely deleted? Are there mechanisms to remove the data from parties who did not consent without jeopardising the validity of the data for research purposes?

When someone deletes a Tweet or digital record, did it really 'go away'? We can extend this point using Twitter as the case. There are many times someone tweets something embarrassing, then deletes it only for it to live on in cached or screen-grabbed form on the internet. At a basic level, when we or any other researcher who does survey research captures data in a digital format or transfers responses from paper to digital format, the data cease to be something that can be destroyed in a physical sense. Compounding this, scientific publishing increasingly requires replication data to be publicly available, so once the dataset is online, there is no longer the option of 'deleting' it. In this example though, we as the researchers had full control over the collection of the data, anonymising it and controlling its public release. For vulnerable people who participated in the research, I can have a high degree of certainty that their safety and privacy will be protected even if the data are online.

This certainty decreases when there are third party or automated systems involved in the data collection. If data goes to a third-party server after being collected, how does a researcher know that the data protection and privacy protocols were followed? Especially for researchers working in politically sensitive environments, if your computer is connected to an unsecure Wi-Fi port, a hostile actor can target your laptop and may be able to steal the information from the hard drive (http://werobotics.org). This is critical because metadata behind the front-end data can be an effective tool in identifying who participated in the research, and a motivated actor can easily take advantage of this. Image and sound files, in particular, come with a great deal of information embedded in them. We only need to imagine the problem of compounding effects, if the data, with identifying information intact, is released onto unsecured internet platforms or websites. In effect, there would be no way to delete data that posed direct risks to research subjects, who require anonymity and privacy for their safety.

The OCHA guidelines for responsible data use offer here a helpful mechanism to classify information and to manage its release based on sensitivity of the data and the risk assessment that is made. A similar approach could be developed for IRB purposes (http://werobotics.org). One of the key challenges that arise from digital research is the pace by which new technologies and innovations are developed, and the inability of existing regulatory systems or ethical boards to keep up. This is a problem that IRB faces as well. Second,

Personal Data Collection Risks in a Post-Vaccine World.indb 30 14-10-2022 11:10:25

the pace of innovation also means that the large majority of the population is unable to fully grasp the changes that are happening and the risks or harms that can result from them. For example, many people still fail to consider how uploading large amounts of personal information onto platforms could be used to try to influence their voting behaviours, or that their information is repackaged and sold to third-party data companies.

These are not the only three risks that arise when doing human subjects research with vulnerable communities using digital tools. But they represent three risks that will be ubiquitous to digital, often online, research done at any level of scale. Using these as key examples for further analysis, the following section will explore how and if digital risks and gaps are addressed in ethics and human research subjects training.

## How Does the Concept of Power Help Improve IRBs and Digital Research Protocols Training?

Having addressed three main risk areas, this section asks what gaps exist in human subjects research pedagogy with regard to digital research mediums, and how managing power – as opposed to creating specific technical guidelines – can help IRBs navigate digital human subjects research. Particularly in the social sciences, much of the curricula focuses on interpersonal processes – the importance and process of gaining informed consent, privacy and anonymity, and risk management when working with vulnerable or traumatised respondents. Power is very directly addressed in this traditional research mode – the researcher, by virtue of knowing more about the project and empirical strategy, has power over the research subject. Recognising these interpersonal dynamics is critical to doing ethical human subjects research, but what is lacking for a research space that is increasingly digital is training on how multidirectional power manifests across different tech actors. This does not mean that training on the interpersonal components of ethical research is unnecessary; indeed, the issues around power differences and ethics between researcher and subject demand their own reassessment in a digital research space.

One of the challenges facing IRBs when it comes to new innovations and technologies is linked to William Oburn's cultural lag theory. Ogburn posits that when changes happen to a system or society, there is a period of time between the diffusion of the new technologies and when the people in the system adapt their behaviour to using these technologies. This lag or 'period of maladjustment' means that for a period of time, there is a gap in how one (a society, system, institutions) adapts to technological changes.

Personal Data Collection Risks in a Post-Vaccine World.indb 31 14-10-2022 11:10:25

This 'period of maladjustment' is one that is often rife with possibility for social conflict as the people who lead the change are faced with resistance by those lagging behind.

Langdon Winner (1986) reflects on a couple of points that are helpful to ponder as we evaluate the relationship between digital communication technologies and a modern-day IRB and research ecosystem. Winner (1986, 25) writes that 'In our accustomed of way thinking, technologies are seen as neutral tools that can be used well or poorly, for good, evil or in between.' Winner argues that technologies do not escape from our social interactions and indeed 'enhance the power, authority, and privilege of some over others'. Deploying digital technologies for data collection purposes inevitably adds a new layer to the power dynamics between the researcher and the research participant(s). Kimball Marshall (1999, 83) extends this point further and notes that 'technology is purposive. It is applied to achieve a goal'. He makes a point to distinguish between technology and science in that 'science seeks knowledge while technology applies knowledge to the manipulation of the natural world to achieve a goal'. Daniel McCarthy (2013) argues that we need to look at how technologies influence social systems through time, arguing that different technologies have different impacts on communities depending on their status and power. This is an inherent dilemma that researchers normally face but which will continue to grow as a problem with further deployment of remote sensing techniques for data collections.

Read, Taithe and Mac Ginty (2016, 1324) highlight similar concerns when it comes to data collection, noting that 'data technologies serve themselves first and foremost, but they also empower their supporters. […] The most significant empowerment that data technology risks bringing is that of those who believe in the potential of technology'. In other words, data collection empowers those who lead the projects or initiatives to the detriment of those whose data are harvested. The promise of technological improvement may, therefore, not be all that it seems.

Problems of power distribution and impact of these technologies are articulated by David Chandler (2015) as he notes the limits of the promise of technological innovation. Chandler writes that 'Big Data does not seem to be very empowering for those who most need social change'. Rather it allows you to be aware of your realities, of the circumstances you are in and reveal the limitations of your current position. Chandler seems to articulate that change is limited to those already powerful and in positions to be able to maximise the utility of these functions. These are important questions for researchers engaged in remote sensing work to address, and for IRBs to evaluate.

Personal Data Collection Risks in a Post-Vaccine World.indb 32 14-10-2022 11:10:25

IRBs also will have to reckon with what Couldry and Mejias (2018) describe as 'data-colonialism', that is the practices and behaviours of organisations that resemble the 'predatory extractive practices of historical colonialism with the abstract quantification methods of computing'. Algorithms and computing techniques are increasingly used to turn social and human relations into data points that are of value for private firms (marketing, advertising, etc.) and governments, which can use them for security purposes (tracking and monitoring, social credit, etc.). These models are extractive and predatory in nature because the individuals whose data are being collected are unaware of the extent and scale to which it is being done (to them), and the scale to which their everyday life has been commodified.

Madianou (2019) introduces 'technocolonialism' as a manifestation of this phenomenon in the relationship between humanitarian organisations and the populations that they look to serve, highlighting a digital inequality that exists between the two of them. Madianou notes that technocolonialism reinforces extractive behaviours in the humanitarian sector and furthers inequalities, as refugees and aid recipients continue to generate new data, which in turn generates new value for organisations and private firms who benefit from them. Data or technocolonialism concerns call for an approach that is critical of this power and the extractive behaviour and processes and allows us to begin to deconstruct and resist data colonialism. Ricaurte (2019) points to the critical role that the state and, for the purposes of this chapter, universities play in systematically reinforcing this model. Ricaurte highlights the need to consider new data governance and data regimes that would ensure rights for individuals and reduce digital inequality. Increasingly there are calls for a new Belmont Report that would articulate new rules and regulations that incorporate the pressing need to tackle the risks and new challenges IRBs face from the use of digital data for research (Raymond, 2019).

What is important, though, is to understand how using digital media in the research process reshapes the basics of ethical research practice. These changes take place in both technical and legal spaces, which are often not covered in traditional ethics training but are central to understanding the ethical and duty-of-care risks that arise when using digital tools. The following sections will map the traditional components of research ethics and human subjects protocols onto the aligned digital technical and legal issues researchers need to be aware of when developing a protocol.

We can start with the traditional issue of informed consent. The legal implications represent the most direct issue. From a legal standpoint, the researcher is laying out to the research participants to what they are agreeing to participate. Under normal circumstances, for example, when doing a survey study, the researcher can easily state that the data will be collected

Personal Data Collection Risks in a Post-Vaccine World.indb 33 14-10-2022 11:10:25

and used in a certain way. They can explain how it will be transferred from paper questionnaire to a .csv file, then used to write an academic article. This is easy because the researcher has multiple tangible ways to show the participants what they are consenting to; this could include showing them the survey instrument, where the .csv file will be stored and secured on a computer, and an example of a journal article, and so on.

A large-scale research project, such as the Heinsberg study in Germany, which created a randomised representative sample of respondents from the 'ground zero' of Germany's COVID-19 outbreak, serves as an analogue example around which we can evaluate the challenges of going digital. The research team essentially turned a district in Germany into a laboratory, observing infection rates among the representative sample of respondents to create an estimate of the total number of infections in Germany (Streeck et al., 2020). This was all done face to face, with biological samples taken from residents of Heinsberg. In this situation it is relatively straightforward to obtain consent. But what if a researcher wanted to use passively collected digital information, such as mobile phone location data, or cameras that could track the body temperature of a subject?

It gets harder when a piece of digital software is used that requires accepting a 'terms of use' agreement that the researcher did not write. In this case, it is important to provide some basic training on the legal principles behind terms of use and how to make them understandable to research subjects.

Consent has technical implications too. As mentioned in the previous section, autonomous and sensing tools create particular risks to informed consent. This can be managed with basic training on how sensing systems work, what happens between the sensor and the server to which it sends data and how the chain of data custody from sensor to researcher is managed. Following the example of training in the basics of understanding terms of use, basic training in how data are transferred from remote location to server to researcher can go a long way in helping researchers clarify what happens to the data that vulnerable communities are providing them. This could include introductory training on server software and the operation of wireless data transfer systems. The idea is not to turn a researcher into a software engineer, but to give them the technical knowledge to understand what is happening at the data collection point so they can clarify it to the research subjects.

This kind of technical training extends into the privacy and identity protection spaces, too. As digital technologies become increasingly accessible to non-technical users – for example, out-of-the-box solutions for remote sensing or software packages that provide users with easy

Personal Data Collection Risks in a Post-Vaccine World.indb 34 14-10-2022 11:10:25

front-end systems for gathering 'big data' – the risks to identity and privacy protection increase significantly. One example of privacy risks that can arise from bulk collection of remote sensing data was revealed in a *New York Times* expose on privacy and cell phone data collection. Though cell phone data collected by some carriers are anonymised, through access of public data, individuals can be easily identified and their movements can end up being tracked when the two datasets are combined (Thompson and Warzel, 2019). Basic training that covers tools like VPNs and TOR, and explains what a file's metadata is and how it can be abused, is important. Also important is instruction on the basics of managing data and hardware so that a researcher can guide an IT consultant or colleague through setting up a digital solution that is part of a research protocol.

Another facet of the technical limitation issue involves a third-party software provider that may not have full access or comprehension of the algorithm or technologies that they are developing. Complex algorithm or software that is built over many iterations and years leads to 'black-boxing'. Blackboxing is where the process that leads to the output of the software or algorithm isn't understood and developers are unclear how they've reached that point. A recent example of this was seen with Apple's launch of its credit card business. Individuals with identical information were given wildly different credit limits, and the company's officials were unclear as to why that happened (Vincent, 2019). This is important to digital research because it adds another layer of complication into how we develop frameworks and guidance for researchers regarding how to best ensure that the rights of individuals are preserved, while minimising risk and safeguarding against harm.

Developing deeper knowledge across these technical and legal areas is only a starting point. Traditionally, the sociological side of research ethics has focused on power, and the balance of power in the relationship between researcher and research subject. Digital platforms bring new and complex power issues into play, at times bisecting the chain of data custody and terms of use that exist between the researcher and subject. Software firms themselves bring their own power to a project, since their business models increasingly rely on using data submitted or shared by communities to tailor their advertising and data services offerings. The following section will explore this level of ethics in digital human subjects research, and highlight both the new power dynamics that arise, how technical knowledge can empower researchers to be good stewards of their research subjects' trust, and innovative ways to manage risks when doing digital research with vulnerable communities.

Personal Data Collection Risks in a Post-Vaccine World.indb 35 14-10-2022 11:10:25

## Balancing the Power among Researchers, Their Subjects and Third Parties

The Signal Code developed by researchers at the Harvard Humanitarian Initiative articulates a 'rights-based approach' for collecting data from vulnerable populations. The code creators argue that the focus on rights of individuals is critical to be able to then pursue a needs-based approach, arguing that without establishing rights for individuals, pursuing a needs-based approach may prove to be insufficient, at best, or cause harm, at worst. As such, the Signal Code stipulates that individuals have a basic set of five rights when it comes to data: 'The Right to Information, The Right to Protection, The Right to Data Privacy and Security, The Right to Data Agency, The Right to Redress and Rectification'. The code is developed as a result of increasing reliance on technological tools to capture large data from population in the onset of humanitarian crises. These tools include remote sensing technologies, geospatial information, technologies to capture biometric data and information communication technologies that can collect telephone data. The Signal Code argues that the rights-based approach applies to all users who engage in activities to 'collect, analyze, process, transmit and communicate, share and publish, and support access to information as part of meeting the humanitarian needs of crisis-affected populations before, during, and/or after crises occur', as such, the Signal Code looks to apply a holistic approach for data collection from start to end. The Centre for Innovation offers a holistic approach to development of a data responsibility framework, which established core elements that help build and develop principles, and places ethics around the project. Therefore, all processes and applications build towards an ethical use for data. Another manifestation of responsible data use rights and principles is advocated by the *Feminist Data Manifest-No,* in which there is an emphasis on the importance of contextualisation of risks and harms. The *Manifest* argues that there is a need to understand that developing generalisable rules without accounting for the context of specific individuals, communities or groups would ultimately reinforce inequalities. The *Feminist Data Manifest-No* recognises the need to centre any work on humanity and an appreciation of the individuality of each person.

Identifying technical fixes and training is only part of the solution. These questions and issues do not arise in a vacuum, and the known issues about power balances between researchers and subjects are magnified in a digital space. One major difference between traditional data collection and the use of online digital platforms for collecting data is how data ownership and use are delineated. When a researcher gathers data for a survey on a tablet and

Personal Data Collection Risks in a Post-Vaccine World.indb 36 14-10-2022 11:10:25

transfers it to their computer, they remain the 'owners' of that data. They control how it is stored, replicated and distributed. When a researcher gathers data using a cloud service, social media or third-party instruments for passive data collection, those data often become the property of the technology or software provider. What happens with that data, how it is replicated or released to other parties, is often outside the researcher's ability to influence. Thus, power dynamics and the associated expectations between researcher and subject are magnified: not only might a subject feel compelled to share data, but they would be doing so in a space where their data could be used by a third party in a way that the researcher has little or no power to influence. What digital platforms add to human subjects research are new intermediating layers of power, defined in legal terms by software providers and economic and social terms between researchers and their subjects.

Some of the biggest questions in this space already are being raised in the humanitarian response sector, as NGOs and international organisations increasingly are exploring and entering into cooperative agreements with multinational technology firms. One recent example that has garnered a great deal of interest is Facebook's new cryptocurrency Libra, which is being adopted by global NGOs like Mercy Corps (Cheney, 2019). Deploying such a tool into high-risk environments with vulnerable populations is fraught with ethical and privacy considerations. At a basic level, the data that are inherent to using a platform like Libra is owned by Facebook, which makes its money selling targeted data to third parties. Can an NGO or humanitarian response agency meet its duty of care and its privacy commitments to the communities they serve while also working with firms like Facebook? This is a question that has evolved for over a decade as crowdsourcing, machine learning and digital volunteer groups have become increasingly involved in humanitarian response (Collins, 2013). The academic side of humanitarian research has picked this up as a theme to be studied with application to practice (Sandvik et al., 2014; Read et al., 2016; Hunt et al., 2016), with legal scholars bringing the conversation into closer alignment with the ethical and protection issues researchers face when doing human subjects research with vulnerable communities (Sandvik et al., 2017; Maitland, 2019).

Since researchers have an ethical commitment to protecting respondents' data, which in many cases can run contrary to software providers' goal of selling those data, what are the emerging tools that can be used to balance power between end users and technology firms? One approach is the establishment of data trusts, which are comanaged between citizens, governments and firms. Data trusts can take the form of a fiduciary trust between citizens, government and data firms (Wylie and McDonald, 2018). These kinds of fiduciary agreements give all parties input into how data are used; they are

Personal Data Collection Risks in a Post-Vaccine World.indb 37 14-10-2022 11:10:25

enforceable in different jurisdictions, and they are flexible, while also preventing capture of data by private actors. This can create an ethical, transparent mechanism for storing and using sensitive data, like medical information, that are often collected during human subjects research in vulnerable communities. Indeed, these trusts currently are being explored by the National Health Service in the UK (Mahonic, 2018) as a tool for protecting and managing sensitive data, while training machine learning software. Data trusts are still a concept that is being developed, and different governance entities have different definitions and approaches for understanding them. For this reason, academic researchers and faculty tasked with doing human subjects research training should be aware of what constitutes a trust from a legal standpoint and understand when the scope of a project requires one. Not all research requires a trust or fiduciary arrangement; yet, understanding the model can help researchers develop informed consent protocols and data management processes that are responsive to the risks that come with using third-party software for data collection.

Fundamentally, ethical human subjects research protocols are grounded in an understanding of, and engagement with, power dynamics between researcher and subject. The previous sections dealt with the individual-level factors that arise when using computing mediums to gather data; cases in which the researcher maintained control of the data through the entire process, and the 'terms of use' for the data were directly governed by an informed consent agreement between the researcher and respondent community. In many ways, the current methods of teaching research ethics provide the tools to navigate this kind of digital space and require only some supplementary technical training on managing data across different private platforms. The real power dynamics and complexity take place when integrating third parties into the research process and managing the power dynamics that they bring to the table. This is where formal training in understanding 'terms of use' and digital data management becomes crucial. The researcher in such cases should bring to the informed consent process both an understanding of how they themselves relate to the research subject and their ability to ensure that research subjects understand how their data will be used by third parties. With better knowledge of the overall digital ecosystem, researchers can make better decisions about which software solutions to use and when to stay off digital platforms all together, thus meeting their duty of care and ethical commitments to the potentially vulnerable communities with which they are doing research. There is a critical need to evaluate whether digital products are truly the appropriate solution. Often, the pursuit of digital solutions leads to further complications and risks that are unnecessary and do not provide an added value to the research process. We must be wary of falling into the

Personal Data Collection Risks in a Post-Vaccine World.indb 38 14-10-2022 11:10:25

trap of digital utopianism and pursue a critical lens in how we design research processes and data collection.

## What Does the Digitally Engaged IRB Look Like?

Human subjects research, especially cooperative research that includes participation by international organisations and private sector actors, is increasingly going to reach into peoples' lives as we move further into the digital era. This means that when we think of IRBs, we have to step beyond the notion that they are an entity that deals only with the interests of university-based scientists and the subjects they study in either labs or managed field conditions. While this notion of researcher and researched always came with a power dynamic, it was one governed by a set of legal and ethical principles that were managed technically. Researchers collected their data and had a relationship with the research participant; there was a space for the researcher to explain the risks, and the job of the IRB was to make sure the ethical protocols the researcher developed for managing the relationship with the research subject did this sufficiently. Even in cases of higher-risk research, such as clinical trials or experiments that involved deception, there was space for the researcher and participant to interact face to face during a debriefing. In the digital world, there is so much scope for using digital information provided by people based on the acceptance of a software firm's 'terms of use', that the human relationships where power could be moderated are impossible to maintain.

For a modern IRB, ethics processes that focus on the specific relationship between a researcher and subject are no longer sufficient. Traditional means of ensuring privacy and anonymity in human subjects research are not fit for purpose when working with social media data, for example. Unlike a household survey, where we as the researchers are in control of what gets entered into the database, scraping the data from a platform like Twitter means that potentially identifying information is being used in research involving real people. There may be a digital veneer between the researcher and the subject, but in the end, data provided by a real person is being used in research. Are these data actually the subject's data? Probably not. The data people provide on social media platforms are likely to be the property of the social media firm, once it has been posted. Before even getting to the stage of using data though, there are a number of legal hurdles that have to be negotiated between researchers and software firms.

A good example is the experience Gary King and Nathaniel Persily (2020) shared about getting access to Facebook data on the sharing of weblinks (URLs). They organised this through Social Science One (http://werobotics.org), a global committee of academics working on social science,

Personal Data Collection Risks in a Post-Vaccine World.indb 39 14-10-2022 11:10:25

social media and computing. Even with the combined talent of the best social scientists, law scholars and computer scientists, organising a large Facebook data release that met the needs of Facebook and the needs of researchers was an extraordinarily complex undertaking. Complex statistical techniques favoured by Facebook for anonymising data made the data unreliable for research, so statisticians and legal experts from Social Science One had to then find a technical and legal solution for keeping data anonymous, while keeping it useable. Once there was agreement on statistical, storage and legal issues, Social Science One continued acting as the gatekeeper for the data.

The mix of expertise in the Social Science One community in many ways makes it what a modern digital human subjects review board should be. They have the multifaceted knowledge required to deal with social media firms and assure researchers have the skills to use the data ethically and effectively. This allows them to act on behalf of the Facebook (or other social media) users, who may not be able to directly consent to their online behaviour being used as data for research.

But if Social Science One is the platonic ideal of what effective review and management of large-scale digital data looks like, this also presents a problem. Not every university of research institution has a mix of faculty with the variety of skills Gary King and Nathaniel Persily have brought together. Indeed, many institutions would struggle to make sure all these skillsets were present on their IRBs. So how do researchers with such resource limitations do digital work ethically? A starting place is using tools like the Signal Code as a guide to the questions they and their IRBs should be asking. If researchers start by asking the right questions, and know what those questions are, then they can seek out the experts necessary to evaluate a project. IRBs can do the same thing. Social Science One is not an IRB and, indeed, as part of any request to get access to the data they host, a researcher needs an IRB ethics approval from their home university. Thus, IRBs themselves need to either be upskilling or developing a better institutional understanding of the questions that come into play when evaluating digital human subjects research.

## Conclusions: Shaping a New Approach to Human Subjects Protocol and Ethics Pedagogy

As technology changes the way we do research and makes data from invisible or vulnerable populations potentially easier to gather, the way that ethics and human subjects protocols are taught has to evolve. Researchers and the technology community are increasingly seeing how found data creates risks that traditionally were only seen in face-to-face research, including risks to privacy and safety (Zhang, 2016; Gibney, 2017). Scholars, including Matthew

Personal Data Collection Risks in a Post-Vaccine World.indb 40 14-10-2022 11:10:25

Salganik (2017), are taking on the challenge of evaluating and finding new ways to teach social science research protocols in an increasingly digital research environment.

As digitalisation blurs the lines around what kinds of human subjects protocols are required to protect the identity of research participants, it is increasingly apparent that the social sciences need to prepare researchers with a broader range of technical and legal knowledge. This is especially the case when researchers work with third-party software providers, particularly if those providers use data collected on their platforms for commercial purposes. This is exactly the kind of tension that arises when a study like Heinsberg's COVID-19 experiment moves from face to face to tracking digital footprints. The reality, though, is that a focus on eliminating or managing risks hinges on *knowing* all the risks. With the speed that new technologies and digital research techniques are evolving, this approach to digital research ethics is impractical at best. Every researcher will not have the collection of expertise, such as is represented by Social Science One, available to them. Thus, having references like the Signal Code as ethical guides for understanding the different ways power manifests in digital human subjects research, and understanding how to make sure that power is managed in a way that protects vulnerable participants, will be critical to future research ethics.

Broadly speaking, research ethics is one of many areas of society that is reaching what is referred to in German as an *Umbrück*, which loosely translates as a 'bridging over'. We are on one bank, and the territory behind us contains all the lessons of a pre-digital world. We have to cross over to a world where digital systems are both actively and passively part of our lives. This Umbrück crosses over the space between pre- and post-digital worlds, thereby representing the changes and re-imagining of how we train ourselves to do ethical digital research in vulnerable communities. If we manage it well, ethics and research protocol pedagogy can help us get the most out of using digital tools for research, while lowering the risk of carelessly or accidently putting at risk the people whose lives could be made better through effective scientific research.

## Bibliography

Andrews, S. M. (2017) 'Drones in the DRC: A Case Study for Future Deployment in UN Peacekeeping'. *Intersect: The Stanford Journal of Science, Technology, and Society*, 10(2), 1–10.

Bhatta, B., Saraswati, S., and Bandyopadhyay, D. (2010) 'Urban Sprawl Measurement From Remote Sensing Data'. *Applied Geography*, 30(4), 731–740.

Chadwick, G. L. (1997) 'Historical Perspective: Nuremburg, Tuskegee, and the radiation experiments'. *Journal of the International Association of Providers of AIDS Care*, 3(1), 27–8.

Chandler, D. (2015) 'A World Without Causation: Big Data and the Coming of Age of Posthumanism'. *Millennium: Journal of International Studies*, 43(3), 833–851.

Personal Data Collection Risks in a Post-Vaccine World.indb 41 14-10-2022 11:10:25

Cheney, C. (2019) 'Facebook's Digital Currency Libra: Why Nonprofits Are Joining'. *Devex*. https://www.devex.com/news/facebook-s-digital-currency-libra-why-nonprofits-are-joining-95142. Accessed 25 June 2019.

Collins, Katie. (2013) 'How AI, Twitter and Digital Volunteers Are Transforming Humanitarian Disaster Response'. *Wired*. https://www.wired.co.uk/article/digital-humanitarianism. Accessed 25 June 2019.

Couldry, N., and Mejias, U. A. (2018) 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject'. *Television & New Media*, 2. DOI: 10.1177/1527476418796632.

Gibney, E. (2017) 'Ethics of Internet Research Trigger Scrutiny'. *Science*, 550(7674), 16–17.

Hunt, M., Pringle, J., Christen, M., Eckenwiler, L., Schwartz, L., and Davé, A. (2016) 'Ethics of Emergent Information and Communications Technology Applications in Humanitarian Medical Assistance'. *International Health*, 8(4), 239–245.

King, G., and Persily, N. (2020) 'Unprecedented Facebook URLs Dataset Now Available for Academic Research Through Social Science One'. *Social Science One Blog*. https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one. Accessed 1 July 2020.

Lidèn, K., and Sandvik, K. B. (2016) *Poison Pill or Cure-All: Drones and the Protection of Civilians*. London: Routledge.

Madianou, M. (2019) 'Technocoloniamism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises'. *Social Media + Society*. DOI: 10.1177/2056305119863146.

Mahonic, A. (2018) 'Can Data Trusts Be the Backbone of Our Future AI Ecosystem?' https://www.turing.ac.uk/research/research-programmes/artificial-intelligence-ai/programme-articles/can-data-trusts-be-backbone-our-future-ai-ecosystem. Accessed 26 June 2019.

Maitland, C. (2019) 'Digital Developments: Harbingers of Humanitarian Change?' WRC Research Paper No. 15. https://www.cigionline.org/publications/digital-developments-harbingers-humanitarian-change. Accessed 25 June 2019.

Marshall, K. P. (1999) 'Has Technology Introduced New Ethical Problems?' *Journal of Business Ethics*, 19(1), 81–90.

McCarthy, D. R. (2013) 'Technology and 'the International' Or: How I Learned to Stop Worrying and Love Determinism'. *Millennium: Journal of International Studies*, 41(3), 470–90.

Raymond, N. (2019) 'Safeguards for Human Studies Can't Cope With Big Data'. *Nature*, 568(7752), 277.

Read, R., Taithe, B., and Mac Ginty, R. (2016) 'Data Hubris? Humanitarian Information Systems and the Mirage of Technology'. *Third World Quarterly*, 37(8), 1314–1331.

Ricaurte, P. (2019) 'Data Epistemologies, The Coloniality of Power, and Resistance'. *Television & New Media*. DOI: 10.1177/1527476419831640.

Salganik, M. J. (2017) *Bit by Bit: Social Research in the Digital Age*. Princeton, NJ: Princeton University Press.

Sandvik, K. B., Jacobsen, K. L., and McDonald, S. M. (2017) 'Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation'. *International Review of the Red Cross*, 99(904), 319–344

Sandvik, Kristin Bergtora, Jumbert, Maria Gabrielsen, Karlsrud, John, and Kaufmann, Mareile. (2014) 'Humanitarian Technology: A Critical Research Agenda'. *International Review of the Red Cross*, 96(893), 216–242.

Personal Data Collection Risks in a Post-Vaccine World.indb 42 14-10-2022 11:10:25

Streeck, H., Schulte, B., Keummerer, B., Richter, E., Höller, T., Fuhrmann, C., Bartok, E., Dolscheid, R., Berger, M., Wessendorf, L., Eschbach-Bludau, M., and Hartmann, G. (2020) 'Infection Fatality Rate of SARS-CoV-2 Infection in a German Community With a Super-Spreading Event'. *medRxiv*. DOI: 10.1101/2020.05.04.20090076.

Thompson, S., and Warzel, C. (2019) 'Twelve Million Phones, One Dataset, Zero Privacy'. *The New York Times*. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html?fbclid=IwAR0o6mLT-uKNWdWtnQuww-NeWvse9DsrdYubiV_AT1jqLu_0lxd1eJoQJEw. Accessed 1 July 2020.

Vincent, J. (2019) 'Apple's Credit Card Is Being Investigated for Discriminating Against Women'. *The Verge*. https://www.theverge.com/2019/11/11/20958953/apple-credit-card-gender-discrimination-algorithms-black-box-investigation. Accessed 1 July 2020.

Winner, L. (1986) 'Do Artifacts Have Politics?' In: Winner, L. (Ed.), *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press, 19–39.

Wylie, B., and McDonald, S. M. (2018) 'What Is a Data Trust?' https://www.cigionline.org/articles/what-data-trust. Accessed 26 June 2019.

Zhang, S. (2016) 'Scientists Are Just as Confused About the Ethics of Big-Data Research as You'. *Wired*. https://www.wired.com/2016/05/scientists-just-confused-ethics-big-data-research/. Accessed 26 June 2019.

Personal Data Collection Risks in a Post-Vaccine World.indb 43 14-10-2022 11:10:25