JDSR 6(3) (2024) 187–205

JOURNAL OF DIGITAL SOCIAL RESEARCH

10.33621/jdsr.v6i3.33352

Shadow footprints and the provision of digital behavioral data

A digital civics perspective on psychology research

Estelle Clements[1] **and Marcus Horwood**[2]

[1] Independent Researcher, United Kingdom
[2] Deakin University, Australia

✉ digitalcivics@gmail.com

Abstract

We introduce the concept of shadow footprints as a means of understanding privacy challenges in the information environment. Growing emphasis on the impact of citizens sharing their personal data goes far beyond the individual, with the increased capacity of algorithms to formulate shadow footprints that inform as much about persons absent from data, as persons present. Data extrapolated from small groups have demonstrated robust utility when applied to larger populations. Individuals who have opted to keep their data private, or who have been unaware that data about their private lives has been extracted from the involvement of their fellow citizens from digital behavioral data, suggest the possibility that informed consent has been circumvented, or not fully investigated. This is increasingly concerning when one considers the potential to impact the body politic through behavioral manipulation drawn from such data. These issues must be considered in the context of ethical and litigious standards to inform robust policy frameworks, legal regulation, and the provision of incentives necessary to provide guidance and civic protections, as well as adherence to good ethical practice.

Keywords: data privacy, information ethics, informed consent, surveillance capitalism, Belmont, digital civics.

1. Contextualizing the challenges of data acquisition in the public sector: A digital civics lens

Behavioral research data can be used to impact the lives of all citizens, including those who have expressed their privacy intentions, with serious implications. This work examines the consequences of behavioral data acquisition across the civic sphere, considering the impact of personal data sharing for psychological studies in the public sector. Ethical methodologies and guidelines for behavioral research data are a critical part of all research methodology, yet such methodologies are often under-researched. We argue that by employing digital civics as a lens to contextualise the landscape of behavioral data acquisition we can identify the vulnerability in data sharing for scientific research in the public sector and observe its potential civic complications that can consequently arise across both the public and private sectors. We draw evidence from a range of arenas including law, finance, and foreign policy to highlight the breadth of potential consequences impacting the civic sphere. Reinvigorating the fundamental ethical principles enshrined in Belmont (1978), we explore how offering potential solutions to these issues creates new questions.

Given the integral necessity of data collection to the scientific process, the practices of data's collection, storage, and use, managed through codified ethics regulation have sought to protect and reassure data subjects that they can have relative confidence sharing their personal information, whilst also ensuring that the quality and integrity of researchers' data and practices are sound (Christian, Johnstone, Larkins, et al., 2022). Examples, including informed consent, secure data storage, and the agreement of anonymity, have been useful tools familiar to many researchers. But, even before the increasing ease of information transference and accessibility, and its potential for data breaches, there have long been issues in the data use landscape. Research findings can always be operationalized for purposes other than their initial intended use (not simply in the public sector, but in the private sector also). The need to respond to this long-standing challenge has been enshrined in the Belmont principles (1978) and reflected in contemporary APA ethical guidelines (2017), but the acknowledged value of forethought in research application has become increasingly complex. As technological advancements open new areas of inquiry, improve our accuracy, and open increased opportunities for predictive behavioral modeling and manipulation, increased issues become apparent. Complications in privacy and data anonymization through use of other existing data sources have also been observed (ICO, 2012, p.19). In addition to this, the capacity to create knowledge from a void of data itself, given its connection to other data sources (See Garcia [2017] on "leaking privacy" in the context of revelations that Facebook constructed "shadow profiles") means that further issues in terms of privacy and data consent are surfacing in the scientific landscape. The complexity and speed with which changes occur, particularly where research meets innovative technology, often outpaces the policy or legal precedent, leaving researchers with a dearth of reliable guidance or even conflicting guidance, and is often fraught with deeply held personal opinions. In short, the professional research scientist is frequently left to manage a highly complex, potentially under-regulated, and emotively charged ethical dilemma: data acquisition is required for good psychological research, yet the mere act of this necessary scientific process of data acquisition, and the research springing from it, could result in serious detrimental consequences that the researcher will not be able to control. While this dilemma has long been a recognized part of the Belmont principles, the increasing competence of Machine Learning and potential of Artificial Intelligence in the data environment means that data could be re-identified, and exploited, through fairly straightforward processes. (The ICO's draft guidelines [2021] discuss such re-identification and its associated risks.) Further, the consequences of such data sets in the context of our increasing ability to extrapolate and operationalize information can be used to affect the behavior, not simply of individuals, but also entire demographics and communities. To address this burgeoning arena of challenge, we apply a lens of digital civics, which assists us in understanding current changes in the technological landscape, and how we must consider, not only their application to various processes, but the ways in which these technologies change our concepts of self, and consequently, our behaviors toward ourselves and others (both in individual and communal contexts) (Clements, 2020a). Digital civics is defined as "the rights and responsibilities of citizens who inhabit the infosphere and access the world digitally" (Clements, 2020a; 2017). By appreciating the staggering changes in self-perception that are occurring in the digital age we can gain better vantage of the impact of these new technologies, and the ways in which their use may be affecting our lives and world (Floridi, 2009). This means that civic processes that once seemed quite appropriate, must be rethought, restructured, and redeployed; a process accomplished through consideration of four conceptual resources that help us methodically approach these changes: philosophy, ethics, history, and civic structures (Clements, 2023; 2020a). Using this digital civics lens, we explore the specific processes that use digital behavioral data sets and research in this context. This research asks the key questions: How do our philosophical views of self impact the changing ways we understand privacy? How will our ethical expectations change and how can we ensure our practices effectively address emerging ethical problems? What previous lessons can we draw from to help us address these challenges, and through what contexts do we approach our world? And, how might the structures and codes, such as the Belmont principles, ethical regulations, and even the incentives to adhere to ethical processes, be made more appropriate or effective for our digital age circumstances? (For a more thorough discussion of such questions for shaping digital civics policy initiatives, see Clements, 2023).

2. The shadow footprint: A paradox of civic and personal responsibility in data acquisition

As researchers in the public sector exploring questions in the disciplines of ethics and of psychology, the authors of this paper have observed how Psychological science in the public sector (such as university research, or research funded by a public body) has actively relied on, and encouraged, research participation as an important and responsible civic behavior. But the altruism of citizens to contribute to scientific advancement in the public sector can also create a powerful vulnerability that extends into, or is connected with, the private sector. This is due to the complex inter-relationship of these sectors (broadly discussed below). While public research is made accessible, including to the private sector (a situation further complicated by the frequent use of private sector apps to acquire research data for public sector research) private companies are often protected (ie. by laws protecting trade secrets) from disclosing their own research data or findings. This dynamic sets up a challenging situation with the acquisition of public research data, because, as we will now discuss, sharing personal data can have impacts far beyond the individual who opts to provide their own data, extending to their broader communities and networks, particularly given the convergence of multiple datasets that can be exploited, not simply for what they do say, but also for what they don't. It has been well established that insights about, or the nature of, a sample of a population can be representative of the entire population when seeking to understand patterns or behavior (i.e., analyses of a few may result in insights about many; Jenkins & Quintara-Ascencio, 2020). As such, regardless of the extent of care a single individual may take to protect their privacy, significant insight into other individuals is afforded via the analysis of data belonging to others from the same demographic. This means that traditional mechanisms for personal data protection, (i.e., self-regulation, a lack of sharing personal data, or withholding consent) do not adequately protect an individual from invasive data analysis of their person. Analysis based on others whose data has been made readily available and who possess shared demographic information, traits, situations, and so forth, can provide deeply insightful and highly targeted insights about that individual. In short, a lack of data is still data, and when all, or indeed most, of the surrounding data is present, it's much easier to see the shape of the missing piece: in the case of individuals interacting within a networked, information-rich environment, this allows the formulation of fairly accurate and highly specialized profiles of individuals who, while they may not technically be present in the data environment themselves, can be extrapolated into digital existence by their surrounding data representations. We label this phenomenon, the shadow footprint: a composite of the terms shadow profile (a concept discussed in the wake of the 2012 Facebook data breach in which it came to light that Facebook was in possession of information about individuals that had not been provided by those individuals [See: Garcia, 2017]) and digital footprints (in which an individual's life and movement on and offline can be tracked through their personal data [Sjöberg, Chen, Floréen, et al., 2016]). Shadow footprints are not only the composited development and deployment of information from a single profile, but include the entire interconnected footprint of an individual's composited data increasingly traceable via their informational identity throughout the interconnected online and offline environments. Thus, the footprint includes all the data that can be derived from consensually obtained data, as well as that obtained from instances where consent is not required, as an individual moves throughout the information landscape. These footprints can be described as dynamic (building conceptually on shadow profiles' more static data representations), responsive to changing information (through their integration of more time-dependent data, for example), and pervasively accumulate the experiences of individuals by drawing from a wide range of data sources, and the interplay between those data sources (compounding and integrating their insights). This is made possible by the networked and information-rich environment, and its tracking technologies, that now function in offline as well as online contexts. Able to provide insight, not only as a profile in one digital environment or for a singular service, footprints track users across services, throughout routine activities, able to formulate a picture of daily life; connecting data, not simply through friend groups and location data, but the interplay between services, and from the communally acquired insights from shared demographic information. When such data is conjoined to formulate a shadow footprint, intimate aspects of daily life become revealed in new and extraordinary ways with, what our current knowledge of shadow profiles and digital footprints suggest, would present a potential for remarkable accuracy, and profound insight. Thus, a picture of an individual's life could be elucidated without that individual ever signing up to a service, and never providing consent.

Considering the potential, such data acquisition may feel like a type of theft against people who don't want to share their data. But such unwarranted observations into the intimate data of a person's life are often legal, or at least, not specifically legally prohibited. Fellow people within their own demographic, or simply in close network contact, sharing personal details can unwittingly help to supplement missing information with a high degree of accuracy (see: Garcia et al., 2018 for a discussion of shadow profiles in the context of Twitter users and non-user, which interestingly, comments on predictability of location based on data from Twitter, but applied to contexts of users outside of Twitter: indicative of the potential of such data to formulate shadow footprints). This extends concern about informed consent: as those guarding their data may have taken significant pains to do so, indicating they do not consent to use of their personal data, whilst simultaneously this data may become available to third parties through other means. It becomes a consensual loophole: a phenomenon that should be impossible given the clarity with which individuals may have made their intentions to safeguard their data known. Yet the capacity to acquire data, pair it with other data from multiple sources, re-identify it, and fill in any missing information with what can be gleaned from available (Kosinski, Stillwell & Graepel, 2013) and targeted demographic data (Garcia, 2017), essentially makes available an instrument to acquire private information, circumventing, not only the usual consensual process, but additionally, the very mechanisms that data protection and research laws aim to create. (For a useful visual explanation of this, see the New York Times Privacy Project [Thompson and Warzel, 2019].)

The difficulty is further exacerbated when we reflect on the remarkably small number of people required to provide insights into a demographic, and the capacity to use that demographic data to elaborate on missing information pertaining to an individual's personal circumstances, thereby negating all of the work done by careful, or aware, members of the community to guard data as a vulnerable entity (even when those citizens actively seeking to protect that data represent the overwhelming majority). The insight here is that some members of the public could place the rest of their community at risk by unwittingly providing a stream of psychological insights about a group that even most of those group members may have attempted to keep private. Yet at the same time, these same citizens are encouraged to take part in the sharing of data as important and altruistic behavior (Clements, 2020b). This powerful paradox asserts that responsible citizens are simultaneously expected to guard their data fiercely, as well as share it openly. And this paradox can be witnessed across the spectrum of activities spanning the online and offline environments (that is, the entire informational environment of the digital age: a conjoined world of information that philosopher Luciano Floridi [1999] has usefully termed, "the infosphere"). For instance:

- Citizens should engage in citizen science movements to input and collect data for use in scientific purposes, but this data could also later be used against them without their knowledge (For instance, thanks to LiDAR technology, the photographs we take, can help improve geological understanding, but the sharing of this information can also be used in nefarious ways that can build a picture of the research participant, and when paired with other behavioral data, reveal ways in which they might be effectively manipulated. (For a summary see: Clements, 2020b).

- Citizens should be aware of their legal opportunities under the Right to be Forgotten, yet the protections it offers against secondary use of data, and the mechanisms that will allow consent to be revoked under this legislation are still unclear even to experts (see: Politou et al., 2018, p.9, and Esposito 2017, p.8).
- Citizens offer informed consent, yet become vulnerable when that informed consent is deployed in ways that do not take care to actually ensure citizen's consent is truly informed. This could allow harm to come to citizens by suggesting that citizens were fully aware of consequences when they agreed to data share in the terms of a social service to be able to interact with others online. (For instance, the contractual language and inaccessibility of style and length in many terms and conditions agreements [see: Obar & Oeldorf-Hirsch, 2020]).

While citizens share their data in the hopes of furthering scientific goals in the public sector and achieving a better world and society, they may not always be aware of the ways it may later be used against them, placed into a new context for exploitation, or employed to reveal important details about their fellow citizens, given the data's fiscal or political currency in the private sector. Thus, a privacy paradox for individuals can quickly become a communal vulnerability. We might view this paradox through the insights of Walter Ong (1982), the media ecologist who postulated "second orality", given that media ecology can provide useful insights for digital civics (Clements, 2023), informing our digital age psychological perspectives about the media-rich environment in which we live. Ong (1982, p. 133) explains that a feature of second orality "is the presence of aspects of oral cultures, (such as its communal sense) within the context of a literate society (in which modern concepts of the individual function)" (Clements, 2017, p. 117). The scholar Charles Ess (2010, p. 116), has proposed the concept of "Hybrid Selves" (conjoining individual and relational selfhood) as one response to this conundrum, and it has already demonstrated some utility addressing personal data in public contexts (see Nissenbaum, 2010). Indeed, the challenge of reconciling the responsibilities one has to oneself, with those one has to the group becomes particularly pertinent when we consider the ways in which shadow footprints can also influence our greater community.

3. Shadow footprints and civic structures: Public researchers in a world of surveillance capitalism

Data acquired and studied in terms of key demographics and groups can be used for shaping civic and social, as well as influencing individual, behavior: it is not only possible to maneuver individuals through the social and civic space, but to influence large groups of people, and impact the group dynamics of these spaces as well. When we approach this insight through a digital civics perspective, and consider how such data acquisition and deployment may act upon our underpinning civic structures; such as laws, civic institutions, democratic traditions, or civic bodies we can begin to assess the challenge of such potential change. It's true that new technological processes have tremendous positive potentials (such as the health benefits of IBM's Watson [Chen, Argentinis &Weber, 2016]). But our existent structural challenges and issues also act upon and delineate the influence and activity these new data sets and mechanisms undertake: how we have been conditioned to behave in the civic sphere, and the ideas we take for granted, influence the ways we condition ourselves for the future. Consequently, while new data, and the ideas we extrapolate from it, hold the potential to alter the ways in which we engage in our civic sphere positively, equally, they can simply reinforce dangerous and unjust practices, like systemic racism (Richardson, Schultz, Crawford, 2019), or colonialism (Costanza-Chock, 2018). We must also consider the ways in which public and private interests may overlap in the civic realm, and how such alignments may also become inimical.

In this context, when we consider the potential role of the shadow footprint in this civic arena, we must become aware of, not only the vast potential of data available from our own data disclosures over time, but the revelation of those disclosures on the wider community. To understand how psychological research data may be used in this way, we must understand the increasingly rich data sources acquired by corporations and applied in increasingly vast, and often misunderstood ways, and their vast revelatory potential. We need also consider the wider context in which public sector researchers operate and how their aims and obligations differ from those of the private sector who view such data as an exploitable resource. "Trillions of data points and six million behavioral predictions per second are the surface of a shadow text over which democracy and its demos have no knowledge, no authority, and no control" (Zuboff, 2019a, p. 19). This practice, which the researcher Shoshanna Zuboff describes as "Surveillance Capitalism" (Zuboff, 2019b), creates an "epistemic injustice" in which a small group, driven primarily by shareholder interests and earnings, can exercise control over the civic and social space (Clements, 2022a). The inter-related fiscal issues that sit at the heart of digital technology research into behavior, and civic processes, highlight the ethical conundrums that arise because "it is the surveillance capitalists who occupy the catbird seat in this new world. They know, they decide who knows, and they decide who decides" (Zuboff, 2019a, p. 19). Building on these surveilling concerns, the legal scholar Julie Cohen delves into the practical realities, from an informational perspective, of such surveillance power in the legal-political sphere (see: Cohen, 2019) redeploying this activity more precisely as "informational capitalism" and highlighting the threats it poses to democracy and the democratic underpinnings of the rule of law. As Amy Kapczynski (2020) points out, reviewing Cohen and Zuboff's work "… informational capitalism brings a threat not merely to our individual subjectivities but to our ability to self-govern. Questions of data and democracy, not just data and dignity, must be at the core of our concern today." This is placed into sharp relief when we consider even the most obvious political uses for such data.

Indeed, perhaps some of the most revealing examples of data demonstrating its potential political power and democratic impact have come from location data. An investigative report from the *New York Times* identified how location data could be used to identify protestors, political actors, celebrities, and private citizens; literally tracing them between venues and events, and to their homes (see: Thompson & Warzel, 2019) charting a map of their political influence or democratic engagements. The sale of such data is lucrative and can include purchases from legitimate data location companies, but also leaked data, such as that purported to be stolen from the Shanghai police and sold on the dark web, as recently emerged (Xiong, Ritchie, Gan, 2022). With the capacity to acquire such data sets and feed them into behavioral modelling with the intention of impacting behavioral outcomes, the implications for the body politic are deeply concerning. From manipulating groups of protests, either to action, or inaction, an individual or corporate body with the fiscal power to enact such technologies in conjunction with the insights of psychological research, can hold unyielding power over citizens even without those citizens knowing they are being manipulated. For instance, election manipulation relies on psychological principles, not just group think, but concepts like motivated reasoning, and affective polarization (Nisbet & Kamenchuk, 2018) to create circumstances of belief, such as a candidate's fitness for office based on information that may be heavily edited/altered/or even entirely fabricated, and that has circulated with apparent support within a group of like-minded persons. These tactics work, not only because they are able to convincingly target individuals sympathetic to a particular cause, but because they ensure the circulation of ideas through networks that ensure the likeliest success based on channels of affinity formulating a unified set of social views as they use the power of interpersonal influence (Raven, 2008) to trickle throughout the population and influence the dynamics of a group. Shadow footprints provide increasing amounts of data about individuals leanings, that allow for the formulation of strengthened networks of common purpose, and the manipulation of group dynamics, that can achieve a multitude of aims specified by those who have the information made available by these shadow footprints. This would include, for instance, the surveillance or informational capitalists that Zuboff and Cohen describe, or those with the financial capacity to purchase such data (or wealthy private individuals, or nation states). Surveillance and informational capitalism is about more than just corporate shareholders and earnings, it is about the power to shape global events in aid of these fiscal drives, and the even greater opportunities that power provides, because combining this data with these tactics formulates effective mechanisms that can be deployed in disinformation campaigns, foreign policy contexts, election meddling, and financial manipulation. The recent spate of media content generated about the American Depp/Heard trial, and subsequent interview on that topic given by the analytics company Cyabra (see: Vice, 2022; Fox, 2022; Vanity Fair, 2022), suggests that such tactics could also be deployed in the legal sphere and public life. That is, these tactics can appear in any of the power structures of our civil society.

Consider, for instance, how financial data is reflective, not simply of fiscal interests and sentiment, but of the wider global picture of interconnected behaviors, expectations, and events. Its analysis, increasingly inclusive of the tiniest measurable impacts, can provide a snapshot into global circumstances, trends, and impacting variables, helping it predict later outcomes and behaviors: a trail of influences traceable through digital data, extending from the smallest thunderstorm in the pacific as it impacts crops, to the largescale impact of those crop changes on government spending or stability months or years later. The ability to analyze and explore such data reveals global shifts in markets but could also anticipate human responses to these: how individuals and groups might be moving and behaving, or even how they might be moved to behave. AI systems (or perhaps more correctly, smart algorithms and deep learning) such as Blackrock's Aladdin already show enormous potential (Henderson & Walker, 2020). Meanwhile, in the foreign policy sphere, psychological research data and findings, coupled with new data acquisitions, can raise numerous issues. The capacity to influence political outcomes – to spur action or inaction, circulate re-contextualized information, or pinpoint conspicuous individuals or groups capable of influencing or inflaming strong public opinion and action – is as readily available to foreign powers as it is domestically. This is brought into even sharper focus when we consider the deployment of bots across coordinated networks for political amplification (Schliebs, Bailey, Bright, et al., 2021) or vast stores of data that can be acquired and mined for insights about citizens. A recent Reuters investigation highlighted US government warnings that one company was sending DNA data from women's prenatal tests to China's military (Needham & Baldwin, 2021). As senior Georgetown fellow and former U.S. counterintelligence officer Anna Puglisi commented "When you can combine large amounts of genomic data – including mothers and their unborn children – with their medical data and history, it is really powerful" (Needham & Baldwin, 2021).

The value of specific targeting based on intimate knowledge of individuals, and the psychological ability to identify those most likely to act on the word of an agent provocateur (see, Bradshaw, Bailey & Howard's [2021, p.9] discussion of citizen influencers), play important roles in these activities. In their work on the psychology of state-sponsored disinformation campaigns, Nisbet & Kamenchuk (2018) discuss the myriad psychological mechanisms potentially at work (including: motivated reasoning, affective polarization, identity affirmation, learned helplessness, the role of self-esteem, cognitive and affective reactance, and the continued influence effect). Yet, as they rightly observe, despite the clear emotional and cognitive responses driving these campaigns, an over-abundance of focus on technological functions has shaped understanding on this topic (Nisbet & Kamenchuk, 2018 p. 65). But, it is behavioral datasets providing the tools to remake the map of political influence. From surveillance capitalists to foreign powers, shadow footprints, the deployment of behavioral datasets, the learnings gleaned from this area of research, and the psychological understanding of how these concepts might be deployed to manipulate the body politic in democratic nations, is formulating vast challenges in the sphere of domestic and foreign policy. It also suggests that power acquisition and dispensation may eventually be the sole preserve of those in possession of the wealth to maintain their control over data and its psychological knowledge, and not the ordinary citizens of a democratic nation. A startling revelation when we consider that much of this research, not simply datasets, but also research findings, originate in the public realm and should be publicly owned. Instead, in this context, a capitalist-pseudo-Foucauldian, money-is-

https://doi.org/10.33621/jdsr.v6i3.33352

knowledge-is-power, dynamic can play out: fiscal support of behavioral data research can ensure that data sets remain under the control of private sponsors or political entities. Perhaps similarly to the historical ways scientific research into burgeoning areas of the scientific unknown remained under the control of the Catholic church in a bid to retain social control through the power afforded by knowledge that could be shared with the public only to the extent is allowed control of the demos (Foucault, 1977). Though Zuboff (2019b) separates herself from Foucault, this would seem to support her insights that surveillance capitalists occupy the catbird seat (2019a), but they must also make room, in a game of political musical chairs, for wealthy private citizens and state sponsors. The democratizing potential, touted in the early days of the digital age, seems less realistic in light of these observations. But, that the same civic power structures and challenges now move across the digital landscape should be no surprise given the aforementioned insights offered by digital civics research: that behaviors and structures are consistent on and offline, given the ontological continuity of the informational environment (Clements, 2023; 2020a). It is worth considering that we are, perhaps, dealing less with new and emerging issues, as we are struggling with very old ones (Clements, 2022a) and perhaps suggests that we seek support through reinvigorating underpinning democratic principles instead of taking radical actions that remove our defining democratic traditions. This seems in line with Cohen's suggestions that we must ensure our laws sit in alignment with democratic principles (Cohen, 2019, as cited in Kapczynski, 2019), and with Zuboff's arguments in favor of improved legal codification, as opposed to the removal of such litigation in favor of self-regulated codes of conduct as requested by surveillance capitalists (2019b). A challenge indeed, as "well-funded teams of lobbyists and lawyers … arguing … promising opportunities to bypass new regulatory obstacles" (Zuboff, 2019b pp. 456) await. Before we explore this re-invigoration though, we might reflect on the value of personal data from a less fiscal perspective.

4. The sanctity of personal data in a discipline reliant on personal data: Challenges to the maintenance of ethical practice

One of the challenges is that the value of personal data is not widely appreciated, not only by the general public, but even, often, by professionals. Perhaps, similarly to price not impacting neural mechanisms when using a credit card compared with using tangible cash when making a purchase (the price is 'out of mind'; Banker, Dunfield, Huang, & Prelec, 2021) so too does it appear that potentially, one typically does not consider the true 'price' tied to providing something as intangible as personal data. Indeed, numerous studies have observed that users tend not to understand the privacy implications of their data sharing online (Dwyer, Hiltz, & Passerini, 2007; Acquisti & Gross, 2006; Jones & Soltren, 2005), even after being educated about the risks (Govani & Pashley, 2005). This apparent painlessness of transaction is enhanced by data's apparent lack of value as communicated to the public on a frequent basis: exchanged for use of services to platforms and digital sites, companies often claim their services are "free".

This is particularly important, as digital civics prompts us to consider the impact of the aforementioned ontological continuity of the infosphere on our views: that is, that the conjoined nature of the online and offline environments means that increasingly humans see themselves as informational entities (Floridi, 2005). If we are taught by private enterprise that personal information has little value, we are in effect being taught that we, as persons, have little value. Surveillance capitalist companies can shape the social system of belief by normalising this perspective, continually reinforcing it given the daily basis on which users access their services. Equating free with the exchange of personal data sets up a dangerous psychological dynamic, one that devalues not simply privacy, but the very nature of individual identity, particularly as we need to use our personal information to differentiate ourselves online in a variety of contexts from social, to fiscal, to political (Floridi, 2009, p. 11). In this case, the earlier Ongian paradox is further exacerbated: the necessity of good data is paramount, yet, at the same time, we must find ways that at once approach our privacy concerns while simultaneously acknowledging our communal need to share data (Ess, 2010). The aforementioned concept of hybrid selves (Ess, 2010) has a critical role to play, but can only be successful if we appreciate the critical value of personal information. This being the case, data should be viewed as sacred capital, the most precious resource we have to understand ourselves and our world, and its sanctity, fiercely protected. This is particularly relevant from a psychological perspective, where psychologists overwhelmingly study the effects of intangible latent variables. For example, in effect, there is no thermometer for depression, latent variables can only be measured indirectly and estimated via observed 'symptoms' or indicators. Consequently, this method of measurement is already prone to error due to its indirect nature, thus data clarity and purity of such indicators is crucial. This is why self-reported data studies may be problematic and also why access to data from source is vitally important. Yet often such social science "research has relied on self-reported engagement" (Johannes, Vuorre & Przybylski, 2021). Collaborations between public research institutes and private industry are emerging (for instance, Johannes, Vuorre & Przybylski [2021] researched psychology and video game play with data from Electronic Arts, and Nintendo) but such practices are currently rare.

Such collaborations, or even acquiring corporately owned data from source for public research, can also be hindered because corporations are held to different research standards than public research institutions. For instance, they can collect, process, and deploy data and research findings in ways that do not seem to reflect the same processes required by public research institutions (see: Zakrzewski, 2022). They are also able to change their terms of service, meaning they could prevent use of their data by public researchers. This leaves public research reliant on the good will of those citizens now caught up in, and further entrenching, the aforementioned altruistic paradox of personal and civic responsibility. Meanwhile, these citizens who make the effort to volunteer for publicly funded research studies are not necessarily representative samplings of the public, and their behavior may alter because they know they are being studied (Feest, 2022). This can set up a challenging situation for public-body researchers, in which the cost of ethically sourced data may feel like a reduction in data quality, while objectively better data seems to sit in the hands of companies and corporations whose business involves generating such datasets (Johannes, Vuorre & Przybylski, 2021), whether or not the public understands such datasets have been compiled. It also begs the question, at what point it became acceptable for companies to hold large bodies of data that they may utilize for fiscal purposes, potentially against citizens' best interests, but not to conduct important research for the benefit of our world, our communities, and our humanity?

In universities and research institutes, research funding can and will be suspended if certain ethical principles are not met. But how this is managed within a corporate environment, in which fiscal remuneration may be contingent upon undertaking the sorts of ethical risks that give rise to information-rich datasets, remains to be seen. If a company wants to know how to sell a product, keep users engaged for longer, or coax data or personal information from individuals, then ethical practices are not the aim, but rather fiscal gains, thereby setting up an unfortunate dynamic in which not only is there little incentive to follow ethical guidelines, but it may prove temptingly advantageous not to do so. That is, such guidelines may present a tokenistic burden for goodwill, prompting a temptation to not appropriately declare things that may be "edge research" (research that sits on the "edge" of ethical boundaries. See: Woodfield, 2017). Indeed, such use of tactics, including "dark patterns" and misleading promises of privacy protection are alleged in a current lawsuit brought by four American Attorney Generals against Google (Zakrzewski, 2022). Compounding these ethical issues, private companies can also exert influence into public research via their provision of research funding to university institutions. The further potential of public researchers' concurrent employment by these same companies, means that the role of "ethical public researcher" (that is, someone supposedly independent and acting in the public interest) can quickly and easily be made questionable, potentially acting to allow or inadvertently lend credibility to unethical research, in an act the philosopher Thomas Metzinger (2019) calls the cultivation of "ethical washing machines". Additionally, when the credibility of independent public research is damaged, public trust is compromised in ways that may reinforce or justify the arguments of private enterprise (i.e., that such unethical practices may be justifiable in the interest of efficiency. See, for instance, Kapczynski's (2020:1483-1484) discussion of the use of Kaldor-Hicks criteria).

Meanwhile, the public research sphere is replete with other challenges to its ethical guidelines and conduct. In pragmatic terms, we are simultaneously, too comfortable, and not comfortable enough, with ethical risk. For while we create formulaic ethics processes to encourage consideration from researchers and ensure that processes have some form of public oversight, such processes tend to live and die at the planning stages of research, have few mechanisms for multiple reporting throughout the research process, and often fail to truly engage the real spirit of ethics: rather, they can be seen as one further bureaucratic task in a long series of tick boxes before the "real" research process can begin (For a discussion on these challenges, including the dearth of literature discussing them, see Christian, Johnstone, Larkins, et al. [2022]). At the same time, such procedures can be fearful processes for researchers looking to innovate and may cause concern that their project may be dismissed from an ethics committee without serious consideration, or worse, terminated partway through, if a pioneering strategy raises popular fears, or, potential litigious concerns. Researchers at Yale who revived a pig's brain found themselves at the center of a public ethical debate, despite having clearance and support from their university ethics committee (Farahany, Greely & Giattino, 2019).

We need to find ways of formulating and incentivizing living ethics procedures, not simply in the private sphere, but in the public one too, because a failure to engage with bigger and riskier research in public institutions may directly lead to: a failure to understand the types of research happening in the private sphere; lead good researchers away from public institutions; and result in naiveté about the sorts of practices that such researchers must be aware of.

5. Psychology researchers as ethicists: multi-prong approaches and democratic principles

Returning our focus to the re-invigoration of democratic principles as a means of approaching and incentivizing ethical practice, we advocate a multi-prong approach. For, while digital behavioral data plays an enormous role in these chains of events, we would be mistaken to believe that only by regulation alone would we achieve the necessary outcomes to safeguard society. Equally, it would be a mistake to assign blame for our own ethical responsibilities to the technology itself, circumventing the responsibility we ourselves owe our own behaviors. As we have discussed, at the heart of many of these activities, are human actors, attempting, with specific intention in many cases, to deploy technology to influence the outcomes of events, and behaviors of citizens for fiscal reasons, or citizens, failing to engage with the reality of their data disclosures, this is before we even consider the inadvertent or accidental outcomes of humans engaging in such technology deployment. Democratic principles include concepts like the rule of law, but also require aspects such as the engaged participation of citizens, checks and balances on power, and education.

Psychology, as a field, must assess its role within the greater framework of civic and social interaction, and find ways that its regulations and ethical components can complement and support a comprehensive and consolidated framework in conjunction with other arenas impacted by its research: including the impact of behavioural findings and data on the private sector. Psychological researchers in the public domain must recognize they are fighting a multi-fronted battle in the deployment of their research mechanisms and findings. They must engage with the reality that psychology research is not used in isolation for purely altruistic or theoretical purposes, but has 'real world' applications, and promote multi-stakeholder ethical engagement so that understanding of research impacts can be informed by interdisciplinarity to ensure outcomes are practicable, achievable, and accurate.

But this can only happen if we are frank about the challenges we face. The potential for the public and private spheres to collaboratively approach such issues faces serious obstacles. Indeed, the struggles articulated by ethicists themselves working for private companies are quite concerning and indicative of these collaborative challenges. The high-profile treatment of ethicists, (for instance, Timnit Gebru's contentious departure from Google was widely covered in the press [see Hao, 2020]) damage corporate credibility at a time of developing public awareness into the issues of mass data collection and seem to make such collaborations an apparent impossibility. But equally, we must reflect on the complicated and differing motivations and expectations of ethicists and ethical researchers working in private corporations, and their employers (Moss &Metcalf, 2019). For while the focus of ethicists and ethically responsible researchers is to discuss and draw out ethical concerns, corporate governance in a private company is primarily answerable to shareholders. Ethics can fall behind a long line of concerns pragmatic to the everyday running of the corporate entity and its success, and in many countries the legal obligations corporate governance owes its shareholders are interpreted to mean company survival at the expense of other, arguably less foreseeably obvious ethical, concerns. In an environment where competitors are seeking the next breakthrough, the need to drive forward at the expense of ethics, perceived as a potential hinderance to fiscal operations, can be seen as legally necessary: placing ethics and the law at odds. And creating frustrating challenges and misunderstandings between public and private ideas about responsible research practices.

A failure to properly understand how companies operate and their responsibilities to shareholders, and the demands of corporate environments, can result in a failure to think critically about the ways risk might be communicated by ethical researchers within a corporate entity: to be heard not as a philosophical principle, but as a long-term challenge that will detrimentally impact a company's survival and long-term fiscal success. Finding pragmatic ways to incentivize and communicate ethical practice, and to embed it appropriately in ways that mean ethicists are heard, and private entities appreciate their responsibilities beyond short-term fiscal gain, are necessary if real engagement with ethical concerns is to take place, or even to make collaborations between sectors possible. This could include taxation incentives, or published metrics demonstrating corporate responsibility as part of a global index of public ethical values (like the models used in environmental "green accounting" See: UNESCWA, nd).

There are challenges for these responses too. For instance, they require global oversight to prevent companies escaping responsibilities or engaging in detrimental practices by moving jurisdictions, but at least they represent a starting place for engagement. And for collaboration to work, researchers and corporate governance must be able to communicate, so companies must be equally active in this process. This means enhanced protections for researchers (such as whistleblower protections, ensuring that researchers can safely make protected disclosures), and company cultures that actively embrace dialogical communication and feedback processes. Companies will also need to recognize the value of ethics: not only can ethical criticisms prevent future litigious issues, and spur product improvement, they keep the over-arching society on which stakeholders depend in the long-term, alive and functioning.

Oversight too, is critically important. The checks and balances in a democratic society necessitate emboldening and keeping independent, regulatory bodies such as Information or Privacy Commissioner's, and government legal advisors, in order that they may: take action as necessary; provide guidance; encourage transparency; and ensure legal regulations are enforced. And as Cohen (2019) observes, such legal mechanisms must be developed in ways that embolden democratic aims, not serve as means of further entrenching informational capitalist's power. Perhaps one of the greatest challenges in light of Zuboff's revelations about the potential of surveillance capitalists to find ways to circumvent these processes, is to ensure robust mechanisms that can support codified regulation, while simultaneously acknowledging their ethical requirements enshrined in the underlying spirit of the law (Clements, 2022a). Education, citizen engagement, and ethical ideas can assist with this. Identifying and engaging with psychological mechanisms can also be useful (Debatin, Lovejoy, Horn, et al., 2009; Nisbet and Kamenchuk, 2018). Nisbet and Kamenchuk (2018) further identify information and media literacy as an important skill to cope with many of these psychological deployments. Such literacy skills are also a component of the digital civics pedagogy framework (Clements, 2020a; 2022b), that can help approach the challenges of digital extremism and misinformation (Rea, 2022). Digital civics pedagogy also

https://doi.org/10.33621/jdsr.v6i3.33352

advocates civic engagement and participation, supporting citizen's knowledge and empowerment by teaching key skills around good ethical judgement, with the kind of approaches that encourage flexibility, forethought, and empathy from an intellectual perspective to approach novel challenges (Clements, 2022a). Such skills have a long history reaching back to antiquity, suggesting this is an ancient quandary, birthed anew in our digital age (Clements, 2022a). For example, the utility of the concept of 'Phronesis' (or 'practical wisdom') to support the development of solutions to ethical (and even pragmatic) quandaries in the digital age, has been identified by numerous scholars (see Clements, 2023; Ess, 2007; Stern, 1997). Hailing from classical virtue ethics, Ess (2007, p. 15) describes part of its capacity as "precisely the ability to discern what general principles may apply in a particular context – and how they are to be interpreted to apply within that context as defined by a near-infinite range of fine-grained ethically relevant details." The flexibility offered by Phronesis would also seem to respond to the need to keep ethics processes "living", encouraging a sustained concern with the ethical potentials and shifting landscape of research projects. The sustained exercise of such wise ethical judgement using general principles can be a useful supplement for a codified ethical framework, such as Belmont. Additionally, the foresight, to appreciate and anticipate the potential later uses of research, constitutes an important part of the Belmont principles (1978), also present in the updated APA ethical guidelines (2017), by which we are all brought together to appreciate our ethical obligations. But such processes will require the active curation and guardianship of digital behavioral data, and now we finally turn our attention to how such processes might be implemented. Again, this is not so much an issue of updating the Belmont principles, as it is implementing them in ways that are contemporary to our digital age, taking account of real-world ways in which civil structures are increasingly impacted by capitalist entities, and the ways in which the online and offline environments are increasingly conjoined through their informational connectivity.

6. Guardianship and data: The APA's ethical principles revitalized not reinvented

How can we address guardianship issues in ways that will engage with the real-world challenges set before researchers, acknowledging the increasing awareness of political and fiscal control sought through the use of shadow footprints? To expect ethical practices from industry and private entities, surely as academics and research institutes we must lead by example. As our review indicates, the current approaches and frameworks within the digital age need rejuvenation, notably with regard to the impact of 'shadow footprints' that result from large scale data collection and analysis. This is not to say that a new set of values are required to be established, but that they can be supplemented through digital civics insights. For instance, recognition of the Ongian "second orality" we discuss, suggests the need to take the community/individual relationship into account. Indeed, to an extent, the APA's Ethical Principles of Psychologists, core principles (Beneficence and Nonmaleficence[A], Fidelity and Responsibility[B], Integrity[C], Justice[D], and Respect for People's Rights and Dignity[E]) consider the broader impact on communities. Principle B, for example specifies researchers' "professional and scientific responsibilities to society". However, when considering the translation of such principles into practice within academic environments, the emphasis is often overwhelmingly, if not entirely, upon the impact on individuals directly involved with the research being conducted, without consideration of how such a project may impact the broader community. We therefore argue the current principles need revitalization to provide guidance that ensures research has the appropriate ethical considerations from both an individual and community perspective.

We also identified the need for living ethics procedures, and the ways in which principles must be administered through an intellectual perspective, capable of considering the sorts of nuance and novel presentations of challenges that occur in the digital age. Through phronesis, we suggested a means to think critically about the ways in which ethics challenges will be addressed in research development, and the foresight to perceive, advise on, and forestall issues that may arise.

Further, our review indicates the need to not only have the underlying principles outlined, but the provision of specific guidance to support adherence to such principles, particularly in regard to surveillance capitalism: what would be minimally expected, and how would external entities determine the extent by which an entity is in adherence? With the acknowledgement of the broader impact research may have on communities so too must we acknowledge the necessity of methods to keep entities accountable; insisting on transparency in research that may have impacts on citizens, and minimalizing harm to the vulnerable. We therefore argue it is also necessary to ensure those conducting research not only strive to adhere to the five aforementioned principles, but be guided by three key metrics upon the extent by which each ethical principle is followed may be determined: Applicability, Quality, and Transparency.

Applicability describes how broadly the research impacts both individuals and communities, and the extent the project has been tailored, and considerations have been made, to the specific individuals and communities would be impacted. (This addresses the Ongian paradox.) Quality describes the rigor and validity of the processes and practices conducted to ensure the principle is consistently followed by the project team. (This incorporates the concept of Phronesis.) Transparency relates to the extent all practices and procedures are able to be scrutinized and known by those involved with the project, the broader impacted community, independent entities, and the general public. (This provides mechanisms to cope with Surveillance Capitalism.)

Below we provide an example framework on how the five key principles may be considered and assessed when considering different research projects. We note, the provided aspects are examples, and are by no means exhaustive, nor reflective of all necessary considerations needed to be undertaken by a project team. For the full definitions of the principles, please refer to the APA guidelines.

6.1 Principle A: Beneficence and Nonmaleficence Adaptation

To expand principle A for the community, the expected benefits and possible harms likely to occur toward the impacted communities needs to be considered (Table 1).

Table 1. Ethics Principle Beneficence and Nonmaleficence Adaptation

Beneficence and nonmaleficence	
Individual 👤	Community 🌐
Applicability	
The benefits of the undertaking to the participants have broad and important applications within their lives.	The benefits for the demographic/community of interest are broad in application, and complementary to future research across multiple disciplines and studied phenomena.
Quality	
Benefits of the undertaking outweigh possible harm to participants.	The benefits of research outweigh possible harms to represented demographics/impacted communities.
The welfare and rights of participants are safeguarded.	The welfare and rights of the represented demographic/ impacted communities are safeguarded.
Transparency	
The benefits of being involved for the participant are clearly communicated and understood by the participants.	The benefits of toward the demographic/community of interest are clearly communicated and understood.

Note. This table only reflects an example of the considerations required for the ethics principle Beneficence and nonmaleficence from the adapted perspective needed in the digital age.

https://doi.org/10.33621/jdsr.v6i3.33352

6.2 Principle B: Fidelity and responsibility

Table 2 reflects how principle B indicates the need for program developers and researchers to specify their considerations and responsibilities toward not only the individuals directly involved with the undertaking, but also the broader impacted communit(ies). Consequent intended and current actions to address such responsibilities are therefore required to be transparent, appropriate, feasible, and rigorous.

Table 2. Ethics principle Fidelity and responsibility adaptation

Fidelity and responsibility	
Individual 👤	Community 🌐
Applicability	
The specified responsibilities and expectations of the researchers are tailored specifically toward the project design and the participants involved.	The specified responsibilities and expectations of the researchers are tailored specifically toward the represented demographic/impacted communities.
Quality	
A hazard analysis and risk mitigation considerations have been conducted and published associated with the research project and participants.	A hazard analysis and risk mitigation considerations have been conducted and published associated with the represented demographic/impacted communities.
Remedies for potential trauma to participants are pre-emptively considered and associated resources appropriately made readily available.	Remedies for potential trauma to impacted communities as a result of the research are pre-emptively considered and associated resources appropriately made readily available.
Systems of data storage and protection are of the highest standard appropriate for the research project.	
Transparency	
The responsibilities and expectations of the researchers are clearly communicated to participants.	The responsibilities and expectations of the researchers are clearly communicated publicly.
Request for information, concerns and complaints by participants can be easily made	Request for information, concerns and complaints by the community can be easily made.

Note. This table only reflects an example of the considerations required for the ethics principle Fidelity and Responsibility from the adapted perspective needed in the digital age.

6.3 Principle C: Integrity

Considerations and consequent actions regarding the how researchers can ensure they act with Integrity, and how they may be kept accountable, are indicated in Table 3.

Table 3. Ethics principle Integrity adaptation

Integrity	
Individual 👤	Community 🌐
Applicability	
All those involved with the research project act with accuracy, honesty, and truthfulness with their conduct.	Data are used in a manner specified when it was initially collected, or further permissions by representative bodies for the demographic/impacted communities is sought.

https://doi.org/10.33621/jdsr.v6i3.33352

Quality	
Participants are well informed and told the truth to the extent the research allows. Any required misleading aspects of the research design toward participants are required to promote the integrity from the global perspective, and do not disregard any other principle component (e.g., beneficence, dignity) to the individual participants.	Published materials are accurate and drawn conclusions are rational and have merit. The methodology, and outputs, are peer reviewed by independent and appropriate experts. Any required misleading aspects of the research design toward the represented demographic/impacted communities are only permitted in order to promote integrity from the global perspective, and do not disregard any other principle component (e.g., beneficence, dignity).
Transparency	
Participants are aware of how their data will be used. Systems of data storage and protection are detailed and provided to participants. Any misleading conduct, part of the research design or otherwise, must be communicated with the participants at the earliest feasible time.	Conflicts of interest are identified, well communicated, and appropriately mitigated/addressed. The methodology adopted, and data collected is made available to the general public within reason, and independently peer reviewed by those appropriately qualified.

Note. This table only reflects an example of the considerations required for the ethics principle Integrity from the adapted perspective needed in the digital age.

6.4 Principle D: Justice

Table 4 reflects how researchers may adhere to the Justice principle across the three key metrics.

Table 4. Ethics principle Justice adaptation

Justice	
Individual 👤	Community 🌐
Applicability	
Anyone meeting the selection criteria has the same right/opportunity to participate in a study, and/or opt out of participation at any time of the project.	Represented demographics/impacted communities have a right to be involved in and benefit from conducted research projects.
Quality	
Researchers exercise reasonable judgment and take precautions to ensure that their potential biases, the boundaries of their competence, and the limitations of their expertise do not lead to or condone unjust practices toward participants. Strategies and procedures are put in place to reduce barriers for individuals to be involved in the project.	Researchers exercise reasonable judgment and take precautions to ensure that their potential biases, the boundaries of their competence, and the limitations of their expertise do not lead to or condone unjust practices toward communities/demographics. Strategies and procedures are put in place to reduce barriers for communities/demographics to be involved in the project.
Transparency	
Researchers make significant efforts to advertise to all eligible individuals regarding involvement in a project, and the associated benefits.	Researchers make significant efforts to advertise to all relevant communities and demographics regarding involvement in a project, and the associated benefits.

Note. This table only reflects an example of the considerations required for the ethics principle Justice from the adapted perspective needed in the digital age.

6.5 Principle E: Respect for people's rights and dignity

And Table 5 provides an example of indicators associated with adhering to the respect for people's rights and dignity principle across the three key metrics.

Table 5. Ethics principle Respect for people's rights and dignity adaptation

Respect for people's rights and dignity	
Individual	Community
Applicability	
Concerns and/or input by participants are legitimately considered, with researchers being open to changes in methodology or procedure as a result.	Represented demographics/impacted communities have a right to be involved in the development of, or oppose and prevent such research on legitimate grounds of lack of dignity.
Quality	
The rights and dignity of participants are considered from multiple facets, especially those not directly tangible to those involved. Privacy, confidentiality, and self-determination of participants are respected, with design targeting procedures specific to their value and maintenance. Adherence to the ethics principles is the highest priority of the researchers to the participants above any of their other interests.	Representative bodies for those being studied, in addition to expert in the area peer review the study methodology to ensure the rights and dignity of those being represented/communities impacted is maintained. Privacy, confidentiality, and self-determination of communities/demographics are respected, with design targeting procedures specific to their value and maintenance. Adherence to the ethics principles is the highest priority of the researchers to the communities/demographics above any of their other interests.
Transparency	
Considerations of how the rights and dignity are made and clearly communicated to all participants. Any breach to a participant's privacy, confidentiality, and/or self-determination is well communicated with those affected, the entity conducting the project, and procedures for remedy are not only shared but promoted with guidance.	Considerations of how the rights and dignity are made are clearly communicated within published material, and consulted with representative groups prior to commencement of research. Any breach to a community or demographic's privacy, confidentiality, and/or self-determination is well communicated with those affected, appropriate representative bodies and legal organisations, and procedures for remedy are not only shared but promoted with guidance.

Note. This table only reflects an example of the considerations required for the ethics principle Respect for people's rights and dignity from the adapted perspective needed in the digital age.

7. Impossible questions: Balancing risks and benefits

At the heart of these ethical risks brought about by shadow footprints, are a series of inconceivable questions, almost beyond imagination. Without convincing answers, how can we approach these issues, particularly as science relies on good data? To find ways of balancing risks and benefits to the unknown, we have employed a digital civics lens to take account of the ethical issues in psychological researched raised by digital technologies, strongly rooting our responses in a framework founded in a philosophy that appreciates the digital age. With reference to the philosophy of information, and in acknowledgement of the ontological continuity of the informational environment (that is the conjoined online and offline spheres) in which these interactions take place, we have raised ethical issues with consideration of ethical obligations and potential ethics-based solutions, like Phronesis. Approaching history, we have recognized the utility of media ecologist Walter Ong, as a means of exploring the relationship between communal and individual responsibilities. We have also identified that regulatory confusion and the challenges raised by new digital processing mechanisms, may enshrine undesirable elements of our underpinning civic belief systems and structural inequalities, particularly through surveillance capitalism.

We have observed how psychological research (including public and private sector data and research findings) provide some of the richest and most important insights about human behavioral functioning responsible for our success and survival, but these same qualities mean it sits at the core of ethical conundrums, provides the tools for foreign and domestic interference, and enables the processes of surveillance capitalism. We have noted that addressing these challenges requires an interdisciplinary understanding from researchers, universal investiture and responsibility, and will require a multi-prong approach to be successful. From this perspective of fairness and justice, it became apparent that a deployment of reinvigorated democratic principles can assist: from greater public education and participation (digital civics pedagogy, multi-stakeholder involvement) to checks and balances on power (incentivization, regulatory bodies, and codes of conduct), including a bolstering of the rule of law (improved regulation and policy). We advocated that democratizing the psychological research sphere might be less about revolutionizing the space through the radical overturning and replacement of our existent framework, and more about galvanizing the underlying principles that guide a fair and judicious program of research and application, making them appropriate and responsive to our digital age. Responding to these insights, we explored ways that the APA guidelines, drawn from the Belmont principles, might be further supported, and offered a set of specified provisions in keeping with these practices.

While shadow footprints present a series of challenges, both new and old, to the research environment, and indeed civil society, we are not without tools to address them. As researchers we must be ethical and intelligent in our research processes, and we may do well to remember that the goal is not an unattainable perfection, but our utmost sustained ethical effort.

Funding statement and acknowledgments

The authors have no funding or competing interests to disclose.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. PET 2006. https://privacy.cs.cmu.edu

APA. (2017). Ethical Principles of Psychologists and Code of Conduct (2002, amended 2017) https://www.apa.org/ethics/code/ethics-code-2017.pdf

American Psychologial Association: http://apa.org/ethics/code/index.html

Banker, S., Dunfield, D., Huang, A., & Prelec, D. (2021). Neural mechanisms of credit card spending. *Scientific Reports*, 11(1). https://doi.org/10.1038/s41598-021-83488-3

Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. (1978). National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. [Bethesda, Md.]: The Commission. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

Bradshaw, S., Bailey, H., Howard, P. (2021). Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Oxford, UK: Programme on Democracy & Technology. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/02/CyberTroop-Report20-Draft9.pdf

Chen, Y., Argentinis, JD., Weber, G., (2016). IBM Watson: How Cognitive Computing Can Be Applied to Big Data Challenges in Life Sciences Research. *Clinical Therapeutics*, 38(4), p.688-701. https://doi.org/10.1016/j.clinthera.2015.12.001

Christian, K., Johnstone, C., Larkins, J., Wright, W. (2022). Seeking Approval from Universities to Research the Views of Their Staff. Do Gatekeepers Provide a Barrier to Ethical Research? *Journal of Empirical Research on Human Research Ethics* 17(3), p. 317–328. https://doi.org/10.1177/15562646211068316

Clements, E. (2023). Exploring Digital Civics: a Framework of Key Concepts to Guide Digital Civics Initiatives. *Philosophy & Technology*, 36(2), 21. https://doi.org/10.1007/s13347-023-00614-x

Clements, E. (2022a). Theuth, Thamus, and digital civics: Plato's formulation of memory and its lessons for civic life in the digital age. *Memory Studies*, 15(4), 767-783. https://doi.org/10.1177/17506980221094516

Clements, E. (2022). Asking Dorian Gray for a Digital Civics Education. Journal of Literacy and Technology, 23(2). https://literacyandtechnologyorg.files.wordpress.com/2023/08/jlt_v23_2_clements.pdf

Clements, E. (2020a). A conceptual framework for digital civics pedagogy informed by the philosophy of information. *Journal of Documentation*, 76(2), 571-585. https://doi.org/10.1108/JD-07-2019-0139

Clements, E. (2020b). Tech, Ethics, and the Digital Citizen. *Geoscientist*, 30(10), 16-17. https://doi.org/10.1144/geosci2020-116

Clements, E. (2017). Digital Civics in Pedagogy: A Response to the Challenges of Digital Convergence in the Educational Environment. Doctoral thesis, Dublin Institute of Technology. https://doi.org/10.21427/D7J45F

Cohen, J. (2019). *Between Truth and Power: The legal Constructions of Informational Capitalism*. Oxford University Press. https://doi.org/10.1093/oso/9780190246693.001.0001

Costanza-Chock, S. (2018). Design justice, AI, and escape from the matrix of domination. *Journal of Design and Science*. https://hdl.handle.net/1721.1/123083

Debatin, B., Lovejoy, J., Horn, A., Hughes, B. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, *Journal of Computer-Mediated Communication* 15(1), p. 83–108, https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," Proceedings of AMCIS 2007, Keystone, Co. http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf

Esposito, E. (2017). Algorithmic memory and the right to be forgotten on the web. *Big Data & Society.* Epub ahead of print 17 April. https://doi.org/10.1177/205395171770399

Ess, C. (2010). The Embodied Self in a Digital Age: Possibilities, Risks, and Prospects for a Pluralistic (democratic/liberal) Future? *Nordicom Information,* 32(2). https://www.nordicom.gu.se/sites/default/files/kapitel-pdf/319_10%20ess.pdf

Ess, C. (2007). Cybernetic Pluralism in an Emerging Global Information and Computer Ethics. *International Review of Information Ethics*. 7. https://doi.org/10.29173/irie11.

Farahany, N., Greely, H., Giattino, C. (2019). Part-revived pig brains raise slew of ethical quandaries. *Nature*. 568, p. 299-302. https://doi.org/10.1038/d41586-019-01168-9

Feest, U. (2022). Data quality, experimental artifacts, and the reactivity of the psychological subject matter. *European Journal for the philosophy of science*. 12, 13. https://doi.org/10.1007/s13194-021-00443-9

Floridi, L. (2009). The information society and its philosophy. *The Information Society* 25(3): 153–158. https://doi.org/10.1080/01972240902848583

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology* 7: 185–200. https://doi.org/10.1007/s10676-006-0001-7

Floridi, L. (1999). *Philosophy and Computing: An Introduction.* Routledge. https://doi.org/10.4324/9780203015315

Foucault, M. (1977). *Discipline and Punish*. London: Allen Lane.

Fox, (2022). Johnny Depp v. Amber Heard: Nearly 11% of Twitter accounts participating in discourse are fake. https://www.foxnews.com/entertainment/johnny-depp-amber-heard-twitterfake-users

Garcia, D., Goel, M., Agrawal, A.K., Kumaraguru, P. (2018). Collective aspects of privacy in the Twitter social network. *EPJ Data Sci*. 7, 3. https://doi.org/10.1140/epjds/s13688-018-0130-3

Garcia D. (2017). Leaking privacy and shadow profiles in online social networks. *Sci Adv.* 4, 3(8):e1701172. https://doi.org/10.1126/sciadv.1701172

Govani, T., Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. Carnegie Mellon. http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Hao. K. (2020). We read the paper that forced Timnit Gebru out of Google. Here's what it says. *MIT Technology Review*. December 4. https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paperforced-out-timnit-gebru/

Henderson, R., Walker, O. (2020). BlackRock's black box: the technology hub of modern finance. *Financial Times.* https://www.ft.com/content/5ba6f40e-4e4d-11ea-95a0-43d18ec715f5

ICO (2021). Introduction to Anonymisation: Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. Information Commissioner's Office. UK. https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-firstchapter.pdf

ICO (2012). Anonymisation: Managing Data Protection Risk Code of Practice. Information Commissioner's Office. UK. https://ico.org.uk/media/1061/anonymisation-code.pdf

Jenkins, D., Quintana-Ascencio, P. (2020). A solution to minimum sample size for regressions. *PloS One*, 15(2), e0229345. https://doi.org/10.1371/journal.pone.0229345

Johannes N., Vuorre M., Przybylski A. (2021). Video game play is positively correlated with well-being. *Royal Society Open Science*. 8202049202049 http://doi.org/10.1098/rsos.202049

Obar, J.A, & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, Information, *Communication & Society* 23:1, 128-147. https://doi.org/10.1080/1369118X.2018.1486870

Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. (White Paper.) https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf

Kapczynski, A. (2020). The Law of Informational Capitalism. *The Yale Law Journal*. https://www.yalelawjournal.org/pdf/KapczynskiBookReview_iqh4qxtw.pdf

Kosinski, M., Stillwell, D., Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the national academy of sciences* 110(15) p. 5802-5805. https://doi.org/10.1073/pnas.1218772110

Metzinger, T. (2019). Ethics Washing Machines Made in Europe. Tagesspiegel. (Translated from German by Safari).https://background.tagesspiegel.de/ethik-waschmaschinen-made-ineurope?__cf_chl_tk=q7b1e62R9K2q.nM4XVkygD2IUc3BWEKhyotYgtJ.DAA-1658848248-0gaNycGzNB70

Moss, E., Metcalf, J. (2019). The Ethical Dilemma at the Heart of Big Tech Companies. *Harvard Business Review.* https://hbr.org/2019/11/the-ethical-dilemma-at-the-heart-of-big-techcompanies

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press. http://www.sup.org/books/title/?id=8862

Needham, K., Baldwin, C. (2021). China's gene giant harvests data from millions of women. *Reuters*. https://www.reuters.com/investigates/special-report/health-china-bgi-dna/

Ong, W. (1982). *Orality and Literacy, The Technologizing of the Word*. London and New York: Methuen.

Politou, E, Alepis, E, Patsakis, C (2018). Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions. *Journal of Cybersecurity* 4(1): 1–20. https://doi.org/10.1093/cybsec/tyy001

Raven, B.H. (2008). The Bases of Power and the Power/Interaction Model of Interpersonal Influence. *Analyses of Social Issues and Public Policy* 8: 1-22. https://doi.org/10.1111/j.15302415.2008.00159.x

Rea, S. (2022). Teaching and confronting digital extremism: contexts, challenges and opportunities. Information and Learning Sciences. https://doi.org/10.1108/ILS-08-2021-0065

Richardson, R., Schultz, J., Crawford, K. (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review*. 94. p.192-233. https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

Schliebs, M., Bailey, H., Bright, J., Howard, P. (2021). *China's Public Diplomacy Operations Understanding Engagement and Inauthentic Amplification of PRC Diplomats on Facebook and Twitter.* Oxford, UK: Programme on Democracy & Technology. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/05/Chinas-Public-DiplomacyOperations-Dem.Tech-Working-Paper-2021.1-4.pdf

Sjöberg, M., Chen, H., Floréen, P., Koskela, M., Kuikkaniemi, K., Lehtiniemi, T., Peltonen, J. (2016). Digital me: Controlling and making sense of my digital footprint. In *International Workshop on Symbiotic Interaction* p. 155-167. https://doi.org/10.1007/978-3-319-57753-1_14

Stern, P. (1997). The Rule of Wisdom and the Rule of Law in Plato's Statesman. *The American Political Science Review*, 91(2), p. 264-276. https://doi.org/10.2307/2952355

Thompson, S. Warzel, C. (2019). Opinion: Twelve Million Phones, One Dataset, Zero Privacy. The Privacy Project. *The New York Times.* https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

UNESCWA. (nd). *Green Accounting*. United Nations. https://archive.unescwa.org/greenaccounting?fbclid=IwAR2ypv0OoUNi2rHKj0Yd02QEGFTPzhMqC_pLoAdf8zU8IqKuvduuO3_UqC8w

Vanity Fair. (2022). What's Really Driving the Memeing of the Johnny Depp–Amber Heard Trial? https://www.vanityfair.com/style/2022/05/whats-really-driving-the-memeing-of-the-johnnydepp-amber-heard-trial

Vice. (2022). The Queasy, Inevitable Johnny Depp Gold Rush Continues Downstream. https://www.vice.com/en/article/epxyn4/youtube-tiktok-johnny-depp-amber-heard-trial

Woodfield, K. (Ed.) (2017). *The Ethics of Online Research (Advances in Research Ethics and Integrity, Vol. 2.)* Emerald Publishing Limited. https://doi.org/10.1108/S2398-601820180000002010

Xiong, Y., Ritchie, H., Gan, N. (2022). Nearly one billion people in China had their personal data leaked, and it's been online for more than a year. CNN. https://edition.cnn.com/2022/07/05/china/china-billion-people-data-leak-intl-hnk/index.html

Zakrzewski, C. (2022). Google deceived consumers about how it profits from their location data, attorneys general allege in lawsuits. The Washington Post. https://www.washingtonpost.com/technology/2022/01/24/google-location-data-ags-lawsuit/

Zuboff, S. (2019a). *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power.* London: Profile Books.

Zuboff, S. (2019b). Written Testimony Submitted to The International Grand Committee on Big Data, Privacy, and Democracy, Ottawa. Standing Committee on Access to Information, Privacy and Ethics (ETHI). (42-1) 152. House of Commons Canada.