



HAL
open science

Ethical research with social media data: informed consent in large-scale quantitative studies

Erwan Moreau, Carl Vogel, Kieran Walsh

► To cite this version:

Erwan Moreau, Carl Vogel, Kieran Walsh. Ethical research with social media data: informed consent in large-scale quantitative studies. Diversity of Methods and Materials in Digital Human Sciences: Proceedings of the Digital Research Data and Human Sciences DRDHum Conference 2022, Dec 2022, Jyväskylä, Finland. pp.200. hal-03912286v1

HAL Id: hal-03912286

<https://hal.science/hal-03912286v1>

Submitted on 23 Dec 2022 (v1), last revised 7 Feb 2024 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Ethical research with social media data: informed consent in large-scale quantitative studies

Erwan Moreau¹, Carl Vogel¹ and Kieran Walsh²

¹ Trinity College Dublin, ² National University of Ireland Galway
moreaue@tcd.ie, vogel@tcd.ie, kieran.walsh@nuigalway.ie

Abstract.

Social media have become a common source of research data, offering high volume, high diversity and ease of access. Nevertheless, beyond the basic legal requirements, the ethics of mining social media data is quite complex. In this paper, we briefly review the state of the art recommendations and propose a specific and practical approach through the example of the Virtual-EngAge project, a project in which computational methods are employed for a quantitative study. In the context of designing this project, we analyze the questions of consent and privacy in detail, discussing the limitations of informed consent in particular. Through the perspective of Information Ethics, we advocate for a holistic understanding of the ethics issues related to using social media users' data, as opposed to the standardized "box-ticking" approach that informed consent forms may tend to favour. We conclude that explicit consent is not always required, in particular if the outcome of the study is in aggregated form, i.e. in such a way that individual data is not released outside its original context.

Keywords: social media, ethics, consent, privacy

1 Introduction

Many studies, especially in the field of Artificial Intelligence (AI), take for granted that public social media data is available for research purposes and does not require any form of researcher-independent ethics review. From a strictly legal perspective, this assumption may actually be correct in many jurisdictions: assuming that the authors of the content are not minor, that the study does not expose any sensitive information and does not put the authors at risk, the study may simply be exempt of Institutional Review Board (IRB) review (Moreno et al., 2013).

However, from an ethics perspective, the literature clearly calls for caution. Social media users may not fully comprehend the privacy issues which could potentially result from making their data public, and they may not appreciate how their posts could be perceived outside their original context. Somewhat paradoxically, given that Twitter users appear to know their postings will be visible to the general public and accept that re-Tweeting is facilitated by the platform, Williams et al. (2017) show that 80% of Twitter users have an expectation that their consent would be asked before their content is republished for the purposes of research. At a deeper level, it can even be argued that the traditional model of informed consent is fundamentally biased (O'Connell, 2016): due to inherent biases in the researcher-participant relationship, it is argued that the information provided to participants has no or little effect on their decision to participate or not. Thus in the context of online data, O'Connell (2016) considers that the procedure of informed consent is actually not designed to

protect the participants, but to protect the researchers and their institution.

The Virtual-EngAge project includes an observational study based on Twitter data, aimed at determining attitudes towards technology among older adults and perceptions held in the community about technological attitudes of the ageing population. The designing stage of the project lead the authors to study the state of the art but also to question some standard approaches to ethics in this kind of study, and eventually to propose a different perspective on the topic.

Thus in this work we briefly review the existing ethics recommendations that have been developed specifically for social media-based research, e.g. (Townsend and Wallace, 2016). Consistent with the unanimously adopted position of the Association of Internet Researchers that the guidelines they suggest are not rules (Franzke et al., 2020), we present our approach to the ethics questions relevant to our project. In this approach, we try to balance the constraints of a small-scale project with these ethics recommendations. In particular we strive to design the study in a way which meaningfully protects peoples' privacy, which gives the participants options with respect to the use of their data, and to the extent possible which anticipates and prevents any form of harm to the participants resulting from the study.

In particular, we argue for strong data availability principles and responsibilities: as long as people make data available for general public consumption (as opposed to privileged consumption, which requires platform membership to inspect) then the data is available for non-harmful research (if people grow roses at the public edge of their front gardens, they have no means of stopping research that depends on counting the publicly visible rosebuds); however, researchers have a responsibility, if requested, to delete underlying data that remains linked to anyone who requests such (an opportunity not available to those whose rosebuds are counted); and people who construct social media data have a responsibility to understand the terms and conditions of social media providers and to be sensitive to public notices of data consumption (that we argue) researchers should provide. That is, as in recent analysis of ethics in active participatory research (Koutsombogera and Vogel, 2017), we emphasize that even passive, "involuntary" research participation entails responsibilities, as well.

This paper is organized as follows: we present the context and the main ethical issues about mining social media data in Section 2. Then we detail our specific approach in Section 3, and finally propose an in-depth discussion about informed consent and privacy in Section 4.

2 Social Media Data: Ethical Issues

From the ethics perspective, the use of social media data for research purposes is a complex issue. (Olteanu et al., 2019, p. 21) summarizes it as the difficulty to reconcile two opposite perspectives: "1) social data research is similar to clinical trials and other human experiments in its capacity to harm people, and thus should be regulated as such; and 2) social data research is similar to other computing research, traditionally focused on methods, algorithms and system-building, with minimal direct impact on people."

On the one hand, one can understandably question why researchers should bother with consent and privacy issues beyond legal requirements, given that private actors (starting with the platforms themselves) do not hesitate to monetize private data. In this naive point of view, since the users' data is already exploited to the maximum extent of the law with very little consideration for the users' privacy or even the indirect harm that this can cause them, the use of the same data for research purposes may seem inoffensive or benign. Furthermore, public social media data may also be seen as secondary data:¹ by definition it has already been collected by the platform which stores

¹Secondary data, in a research sense, is typically collected for a specific, or at least a more defined purpose where the scope of potential uses can be argued to be clearer. Where official statistics and data are used, there is less potential

and publishes it, so it is tempting to assume that the platform is responsible. According to this view, social media data can be used for research purposes without IRB review or through an expedited review process. A large number of studies relying on social media data are published without any form of ethics approval process. This is especially common in disciplines which are not particularly familiar with research based on human participants, like AI, as opposed to social sciences.

On the other hand, researchers' views of ethical use of data should not be automatically benchmarked against the normative standards/values of the industry given differences in goals. There have been a number of works in the literature which specifically study the ethical aspects of using social media data in research, as well as recommendations such as those from the Association of Internet Researchers (AoIR) (Franzke et al., 2020). While institutional guidelines vary widely, there is a consensus in the literature that proper ethical considerations should be carefully studied before proceeding with any study based on social media data. Some of the main principles which guide ethics in research were established in the Belmont Report (US National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1978): respect for persons, beneficence, and justice. Under these core principles, researchers have a duty to consider the potential implications of their research on the participants it relies on. There are many ways in which using social media data could directly or indirectly cause harm to the authors of this content themselves or to others. In particular, researchers often underestimate how difficult it is to safeguard the users' anonymity, and consequently their privacy: even when good faith efforts are made at anonymizing the data, it has been shown that simple investigation techniques, often by crossing the dataset with other sources, can uncover the identity of at least some of the participants, if not all (Zimmer, 2010). This can even lead to disclosing a participant's membership of a minority group, potentially making them a target for various forms of discrimination. One should also be careful about the indirect impact the research results or methods can have. For example, a study demonstrates that individuals of low socio-economic status (SES) are more susceptible to some specific disease; the researchers would probably hope that their result will improve the level of healthcare received by this population, but it might in turn cause private insurance companies to limit their access to health insurance, causing the opposite result. In terms of the responsibility of participants to be aware of these issues and possible data uses, there is asymmetric information availability where those creating/posting this data are not aware of the full intended set of uses (particularly given the rapidly changing capacities of systems), and where there can still be argued a duty of care to participants on the part of researchers.

3 Approach

3.1 The Virtual-EngAge Project

The Virtual-EngAge project aims at tackling the challenges of digital exclusion and limited opportunities for engagement and participation for older people. Although these challenges have become very evident during the COVID-19 pandemic, they represent longstanding issues in Irish and other societies. The project is examining how everyday communication devices (such as telephones, and internet enabled devices e.g. smart phones; ipads, etc) could be used by retirement association groups to strengthen their capacity for supporting their members and others to become socially connected, to access and disseminate critical information, and to advocate on key issues for older people. By doing this the project hopes not only to find new short-term strategies for these groups based on the technologies that they have available, but also inform the development of new and usable technologies that are effective in enhancing these sorts of engagement. Currently, ageing related

to draw out attitudinal inferences or a detailed picture (as in identifiable) of personal circumstances.

technology is often developed without consultation with older people, and does not reflect their needs, preferences or daily lives.

3.2 Methodology

The Virtual-EngAge project includes an observational study based on social media (primarily Twitter) data aimed at determining attitudes towards technology among older adults and attitudes in their context about the attitudes of older adults towards technology. In this part we sketch the methodology designed for this study, taking into account the ethical considerations outlined above.

The scope of the study will be determined by a set of target terms, and the social network Application Programming Interface (API) will be used to extract content relevant to the study. Importantly, the goal of the study does not require any individualized data, only global patterns representative of the general attitudes with respect to the topic. While we seek to separate attitudes *of* older adults from attitudes *about* older adults, we approach this with a level of granularity that does not require knowing which individual professes which attitude. Naturally the processing, cleaning and interpretation of the data necessarily starts with the raw content posted by the users, which may include personal information (for example the Twitter handle, at least).

Thus we distinguish two stages (described below) in the processing of the data. This is meant to clearly identify the status of the data with respect to privacy, and consequently the required level of safeguarding associated with it.

- The **raw data** as it appears at collection stage, which potentially contains personal or possibly even sensitive information. This form of data must be treated with extreme care: during the period of retention of raw text data, this will be maintained in password-protected files on secure computer systems. This is in accordance to the appropriate legislation which are underpinned by the Data Protection Acts 1998 and 2003. This entails the following duties:
 - Obtain and process information fairly.
 - Keep data only for specified, explicit and lawful purposes.
 - Use and disclose data only in ways compatible with these purposes.
 - Keep data safe and secure.
 - Keep data accurate, complete and up-to-date.
 - Ensure that data are adequate, relevant and not excessive.
 - Retain data for no longer than necessary.
 - Give a copy of his/her Personal Data to an individual, on request.
- The **processed data** is a refactored version of the data which does not contain any identifying information. Various techniques will be used to minimize the risk of ulterior personal data collection by third parties:
 - Wherever possible, text content will be represented as “bag of words”, i.e. not in the original word order. This is meant to prevent that an automatic search of a sequence of words would trace back to the online content of the original author. Verbatim quotes of online content will be avoided in publications for the same reason.
 - Specific identifying information in the content, such as persons or locations names, could potentially be used by third parties to retrieve personal data and/or cross it with other datasets. Such information will be removed automatically by filtering out rare words (frequent proper names, e.g. “Ireland”, cannot be used to identify the author).
 - We anticipate that most (if not all) of the published results obtained from social media

analysis will represent aggregated trends in attitude among the observed population, as opposed to individual traits. Therefore, the risk of personal data leakage is low.

The research team will establish a process which transforms the raw data into the processed data. This process should be as deterministic as possible, i.e. preferably automated or following clear guidelines when involving human intervention and interpretation. The guidelines will be established progressively from relevant observations made both in the data and externally, with the objective to make the process reproducible. This is needed to ensure that the modifications to the raw data, in particular the removal of some content required by a participant, does not prevent or hinder reaching the outcome of the process. It is also preferable for replicability purposes,² in order to allow a similar experiment to be conducted on a different dataset. This is especially important since the raw data will not be publicly released, thus making reproducibility by other researchers impossible.

Of course, participants retain the right to opt-out of the study and to modify or suppress their content.³ Only the researchers of the project will have access to the original non-anonymized content (raw data), which will be definitively deleted by the end of the project.

Legally speaking, specific consent is not required because users agreed to the use of their data for various purposes, including academic research, as part of the terms of use of the social media platform. But from the perspective of research ethics, the option to simply rely on the terms of use is questionable. A survey of existing work suggests to follow the ethics recommendations considered the broadest and safest, namely to require participants to sign a consent form. While this option is satisfactory in many cases, it also has significant issues and limitations, detailed in the next section. Thus it was decided for the Virtual-EngAge project to adopt a different approach where consent is not asked but strong measures are taken to protect privacy. In the next section below, we analyse the arguments which led us to this conclusion.

In our view, it is also important from the methodological standpoint that this study is integrated within a broader project, with other strands that capture multiple views, perspectives and lived experiences on the issue. As a mixed-method study, and in overarching terms and in relation to all its methods, it is argued that it benefits from having the considerations and sensitivities of some of the other strands mixed in with decisions around our general approach and design.

4 Discussion about Consent

From a legal perspective, users who post content on social media networks should be aware of the terms and conditions of the platform which hosts their data. In the case of Twitter, users agree to the use of their data for various purposes, including academic research. There is no ambiguity about the legal responsibility of the user; for example, US Courts have confirmed that a person cannot invoke their right to privacy with respect to writings that they post on a social media website, since they made them available to the public by doing so (Moreno et al., 2013).

One principle is that if one accesses data without platform privileges, because the platform and user both make the data public (as through Facebook, perhaps), then the researcher does not have a direct means of contacting individuals, and this distance appears to be appropriate in the context of an observational study. Accessing data with privilege as a member of the platform means that the researcher is more entwined with the prospective research participants, and this seems more com-

²We use the ACM terminology: *reproducibility* refers to redoing an experiment using the same experimental setup, including the same dataset; *replicability* refers to redoing an experiment using a different experimental setup, for instance a different dataset. (Association for Computing Machinery, 2016)

³Explicit requests to opt-out are unlikely, since participants would not usually be aware of the study. However a participant could delete their content from public view (e.g. by changing their privacy settings), and this would have the same effect.

plicated, ethically. The responsibility to communicate directly with participants is greater, and they may be tempted to alter their online behaviour thus causing bias in the study.

Nevertheless, the legal framework is often a vague abstraction for many users. In practice, people often do not read the terms and conditions and sometimes do not even have a good understanding of the privacy and security settings provided by social media platforms (Beninger et al., 2014). As (Williams et al., 2017, p. 1153) mentions, “researchers should not assume all users have read and understood terms of service that govern issues such as consent and privacy”. Moreover (Swirsky et al., 2014, p. 1) emphasizes that “users may not fully appreciate the privacy risks involved in sharing information, and they may therefore experience an online disinhibition effect”. Thus users may feel ashamed or humiliated if their content is taken out of context and scrutinized afterwards. Therefore this could potentially breach the “do no harm” fundamental principle of research ethics.

The major question thus focuses on the extent to which a researcher should protect the social media users when using their data in an experiment, even though the users submitted said data to public scrutiny voluntarily. To phrase the same idea in a somewhat provocative way, is it the responsibility of the researcher to protect the users against their own possible ignorance regarding the service that they choose to use?

4.1 Informed Consent

Traditionally, this problem is answered through a simple consent form: by explicitly asking the participants to consent to the use of their data for a specific and clearly stated research purpose, the researcher can safely assume that the participants have been informed and carry on with their research. While this approach intuitively makes perfect sense and is generally considered satisfactory by ethics review boards, it relies itself on some questionable assumptions.

The principle of informed consent originates from medical research. It was developed as a way to prevent unethical experiments, in the aftermath of some infamous cases of abuse such as the Tuskegee Syphilis Study, from 1932 to 1972. It is established in various international and national legislation, e.g. the Council of Europe’s Convention on Human Rights and Biomedicine.

The fact that informed consent is primarily intended for medical studies is often considered as a problem by non-medical researchers, in particular in social sciences, for several reasons. First, it is clear that the risks are of a different nature when the participants undergo some medical procedure versus when their social media data is analyzed. At a deeper level, “many argue that informed consent protocols reproduce a dominant medical model and a rigid view of power in clinical and non-clinical research.⁴ Universal standards never uncover the material and cultural inequities of research itself (i.e., North–South funding inequities), the problematic assumptions underlying research studies (Western colonial epistemes), and the institutional and organizational practices that configure the researcher and participant role (university vs. community)” (O’Connell, 2016, p. 73). There is a fundamental imbalance of power between the researcher, i.e. an authority figure, and the laypersons asked to consent to some apparently complex research on their data. This bias can cause people to sign a consent form without reading or understanding it, making their consent ethically meaningless, but legally valid. In fact, it has been shown that “providing (too much) information to the research subject can occasionally lead to the opposite effect of what the informed consent aims at; excess of information can leave the concerned party unable to make a (truly) informed choice after all.” (Christen et al., 2016, p. 209).

From this point of view, it can reasonably be argued that informed consent forms are designed to

⁴Of course, in social science research, power imbalances may also exist, as for example in situations in which the researcher conceives of an issue as a problem, but where prospective participants do not all agree that the issue constitutes a problem.

primarily protect the researchers and their institutions, not the participants. Practically, these are used as a legal contract signed by a supposedly rational person, releasing the researchers (and their institutions) from any further scrutiny. As long as the participant signed the form, it is assumed that they have a clear understanding of the goals and risks of the project, even though the information they are provided with has actually very little effect on their decision-making process (O’Connell, 2016). “The normative top-down expression of power ... [imposes] ... a singular standard for consent that is based on the idea that the researcher always has more power and no risk compared to the participant” (O’Connell, 2016, p. 74).

In the context of social media data, there is an irony in asking users to give their consent: this is usually done through a form which explains the research in fairly technical language and explains to the users their rights in legal terms, essentially reproducing the same kind of bias found in the terms of service of the platform. Many users perceive this document as long and full of obscure jargon, and end up not better informed or truly consenting whether they agree or not. Since the motivation for asking their consent was precisely to make sure that they agree assuming that they might not have read or understood the terms of use of the platform, it seems misguided to assume that they would this time truly read and understand the consent form. As a consequence this process is ethically meaningless: if one assumes that users are reasonably careful and rational, their consent to the terms of usage of the platform is sufficient for using their data. If it is assumed that users do not truly understand these, it is extremely questionable to expect them to better understand the research consent form.

Naturally, there are certainly cases where the informed consent plays an important role and duly protects participants. But the standardisation of informed consent processes is sometimes akin to an industrial automation process, i.e where a task previously relying on human expertise becomes “de-humanized” for the sake of efficiency, especially within social media platforms: in this “simplified” approach, the notion of consent is codified and formatted in a way which facilitates a “tick-box approach” to ethics, where instead of considering the diversity of individuals and the various potential difficulties or questions they might raise, their understanding and consent is extremely simplified into a polar interrogative: did they sign the consent form? The Facebook-Cambridge Analytica data scandal⁵ started with a study which duly obtained the “informed consent” of many Facebook users, thus had at least the appearance of ethical legitimacy. The lack of any check or monitoring by Facebook and the dishonest behaviour of Cambridge Analytica show why consent forms on their own do not suffice to make a study ethically valid: real ethics is not a matter of formal “box ticking”, it is a continuous process which requires efforts by the researchers, their institutions and their research communities towards making sure that every step is done in accordance with ethical principles.

Of course, practices widely vary among different fields, institutions and researchers: not every researcher or IRB follows a simplistic approach to ethics, nor is it necessarily prevalent. While this shift in thinking around the nuances and challenges of consent has become evident within certain research fields and institutional research review boards, for example by developing active and iterative consent and assent processes, it can be argued that research concerning social media analytics has remained narrow in its understanding and practices regarding consent.

4.2 Privacy

Asking the participants their consent is meant to fulfill several objectives: their agreement validates the fact that they are aware of the risks for themselves, and of the rights and protections that they are offered. It also confirms their support, or at least their absence of objection, to the goal of the

⁵https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal – last verified May 2022.

study. This can be important in case the study involves a sensitive and/or controversial topic, such as abortion rights or the rehabilitation of former convicts.⁶ When collecting social media data, the main risk to participants and thus the main ethical issue that informed consent aims to address is about their right to privacy, and the harm which can result if their privacy is breached.

4.3 Information Ethics

In this analysis of the question of privacy, we try to apply and follow the principles of Information Ethics (IE) (Floridi, 1999). IE is proposed as a macro-ethic which does not only provide a solid basis for Computer Ethics (the field of ethics applied specifically to issues in the domain of new technologies), but also offers an original perspective by making *information* the main focus of any ethics question. Here *information* should be understood in the broadest sense: “any entity is a consistent packet of information, that is an item that contains no contradiction in itself and can be named or denoted in an information process.” (Floridi, 1999, p. 43). In this perspective, the integrity of the *infosphere* (the information environment) should not be damaged, should be preserved, enriched and nurtured. The author expresses this by proposing four laws (ordered by increasing moral value) which determine whether an action is moral or not. Entropy in the infosphere ought: (1) not to be caused; (2) to be prevented; (3) to be removed. (4) Information welfare ought to be promoted by extending, improving and enriching the infosphere. On this construction, as entities, humans constitute information, as do rosebuds, but facts also supply information, while falsehoods do not. Our view of information ethics is that it provides an imperative to develop information, to study what may be learned from data that is visible in public without privileged access, provided this de-links data from individuals from the analysis and reporting (despite individuals having themselves created a link to the primary data).

4.4 A different perspective on privacy

Privacy is a complex question. (Coll, 2014, p. 1250) argues that the concept of privacy has been “reshaped by and in favour of informational capitalism, notably by being over-individuated through the self-determination principle”. As a result, “privacy becomes only about data and remains the right and responsibility of every individual instead of a collective value.” (O’Connell, 2016, p. 81). In this perspective, (O’Connell, 2016, p. 82) also argues that “concerns about big data sets become a question of data protection, not a question about the ethics of the research question. As a less direct form of data collection, issues of harm and confidentiality appear less critical or are viewed as being already in the public domain.” This is a serious issue, because restricting the concept of privacy masks the fact that ultimately the risk is about harm, and increasingly the risk of causing distress within that. Thus despite an individual’s privacy being protected, if what the individual said or their actions is framed in a way that causes them distress, this is just as problematic.

This concept of data protection stems from the view of privacy as an individual’s right to decide whether they want to retain or release information about themselves. This view assimilates personal data as a *property* of the individual, and naturally the individual is entitled to do as they see fit with their property, similarly to their physical properties. IE offers a significantly different interpretation: it postulates that their information does not only *belong* to the individual, the individual *is* the sum of all their information. Thus any privacy “intrusion is disruptive not just because it breaks the atmosphere of the environment, but because any information about ourselves is an integral part of ourselves, and whoever owns it possesses a piece of ourselves, and thus undermines our uniqueness and our autonomy from the world. There is information that everyone has about us, but this is only our public side, the worn side of our self, and the price we need to pay to society to be recognised as

⁶In the case of the Virtual-EngAge project, it is reasonably safe to assume the goal is not sensitive or controversial.

its members” (Floridi, 1999, p. 53).

In the context of collecting social media data, we propose the following interpretation: social media users post content⁷ voluntarily on a platform. Their action takes place in a specific context, i.e. time and environment (social circle, chances that strangers would see the content, etc.), which defines the boundaries in which the user intends to broadcast this information (whether they are fully aware of these boundaries or not). As a consequence, and given the current inefficiencies and flaws in the process of consent declarations from users, we argue that collecting data without further consultation is ethically acceptable as long as it does not modify the boundaries defined (purposefully or not) by the individual, and as long as a macro-ethic applies regarding data aggregation and dissemination. This implies that their data should not be broadcasted outside the original context. For example, verbatim quotes in a research article should be avoided because they make the identification of the participant easier, since entering the quote on a search engine is usually sufficient to find the original post. Additionally identification should be prevented not only by a random stranger, but also by people belonging to the social circles of the author, e.g. members of their school, work environment, neighbourhood. Instead, all the results should be aggregated in a way such that the original individual content is indiscernible. For example, (Williams et al., 2017, p. 1158) suggests that “quantitative analysis of Twitter data that presents findings in aggregate form (such as tables of regression results, topic clusters in word clouds and anonymised network visualisations) is one way to support ethical research without the need for informed consent.”

4.5 The context matters

Naturally the participants and their potential level of vulnerability and marginality are an essential component of the ethical design of a study. For example, the Virtual-EngAge project is focused on older adults and their attitudes towards technology in Ireland. The general arguments that we put forward in this article apply, but additionally there could be some prejudice in the population around this topic, and a forum such as Twitter is prompt to mock or even insult people for their mistakes. This makes protecting the participants’ privacy (in the sense described above) a priority of our ethics design.

The objectives of the study also matter, in particular the type of information collected as well as the audience susceptible of having access to it. For example, safeguarding the participants’ privacy requires a stronger approach if the dissemination plan involves media outreach and political organizations than if it plans only scientific articles in a few specialized journal.

It is important to emphasize that the authors do not support any approach to the exclusion of all others. On the contrary, like many others we strongly encourage taking the specific context of the study into account in the ethical design, as opposed to adopting any predetermined solution. In particular we acknowledge that multiple other factors can also be taken into account, even though we did not address them specifically in this paper: cultural systems inform ethical values, and the evolving international standards should not dismiss regional interpretations for example.

5 Conclusion

We have argued that the imperative to create knowledge suggests that learning generalizations by aggregating data voluntarily made available to the general public by individuals entails that it is ethical to so study such data. For millennia the imperative to create knowledge has been balanced by

⁷In the IE view, any content that a person posts is *personal information*: even if it does not contain anything about the author themselves, the simple act of posting is itself an information about the individual, and therefore *a part* of the individual.

fear that knowledge can be dangerous and that there are certain things which should not be known. But in these current circumstances, it falls to the researcher to ensure that a macro-informatic ethic is applied to ensure this aggregation is a sufficient abstraction to ensure privacy and freedom from harm and distress. Further work is required within the field to guide and perhaps regulate this aggregation to support researchers in this endeavour.

We argue that provided one abstracts away from the individuals who create data, and eschew identifying individuals in reporting data and generalizations, where people have voluntarily made data visible to anyone in the public who lacks privileged access, it is ethical to study that data without additional consultation. In most cases, it is appropriate for such researchers to provide a similarly unfettered declarations of their research. More sophisticated platforms for such declarations may emerge in the future, and development and innovation work in this regard is certainly required. However, regardless of whether they do or do not, there is a critical need to address urgent ethical questions regarding how knowledge gained through these spheres is applied and disseminated. It is useful to know whether rosebuds are opening earlier each year; it is wrong to use this knowledge to impune individual gardeners.

6 Acknowledgements

This research is supported by the Irish Research Council through its funding to the Virtual-EngAge project (COALESCE/2021/63).

References

- Association for Computing Machinery. Artifact review and badging, 2016. URL <https://www.acm.org/publications/policies/artifact-review-badging>.
- Kelsey Beninger, Alexandra Fry, Natalie Jago, Hayley Lepps, Laura Nass, and Hannah Silvester. Research using social media; users' views. *NatCen Social Research*, pages 1–40, 2014.
- Markus Christen, Josep Domingo-Ferrer, Bogdan Draganski, Tade Spranger, and Henrik Walter. On the compatibility of big data driven research and informed consent: the example of the human brain project. In *The ethics of biomedical big data*, pages 199–218. Springer, 2016.
- Sami Coll. Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance. *Information, Communication & Society*, 17(10):1250–1263, 2014.
- Luciano Floridi. Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology*, 1:37–56, 1999.
- Aline Shakti Franzke, Anja Bechmann, Michael Zimmer, Charles Ess, and the Association of Internet Researchers (2020). Internet research: Ethical guidelines 3.0, 2020. URL <https://aoir.org/reports/ethics3.pdf>.
- Maria Koutsombogera and Carl Vogel. Ethical responsibilities of researchers and participants in the development of multimodal interaction corpora. In Peter Baranyi, Anna Esposito, Péter Földesi, and Tamás Mihálydeák, editors, *8th IEEE International Conference on Cognitive Infocommunications (CogInfoCom 2017)*, pages 277–282. IEEE, 2017.
- Megan A Moreno, Natalie Goniou, Peter S Moreno, and Douglas Diekema. Ethics of social media research: common concerns and practical considerations. *Cyberpsychology, behavior, and social networking*, 16(9):708–713, 2013.
- Anne O'Connell. My entire life is online: Informed consent, big data, and decolonial knowledge.

Intersectionalities: A Global Journal of Social Work Analysis, Research, Polity, and Practice, 5 (1):68–93, 2016.

Alexandra Olteanu, Carlos Castillo, Fernando Diaz, and Emre Kıcıman. Social data: Biases, methodological pitfalls, and ethical boundaries. *Frontiers in Big Data*, 2:13, 2019.

Eric S Swirsky, Jinger G Hoop, and Susan Labott. Using social media in research: new ethics for a new meme? *The American Journal of Bioethics*, 14(10):60–61, 2014.

Leanne Townsend and Claire Wallace. Social media research: A guide to ethics. *University of Aberdeen*, 1:16, 2016.

US National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. *The Belmont report: ethical principles and guidelines for the protection of human subjects of research*, volume 2. Department of Health, Education, and Welfare, 1978.

Matthew L Williams, Pete Burnap, and Luke Sloan. Towards an ethical framework for publishing twitter data in social research: Taking into account users' views, online context and algorithmic estimation. *Sociology*, 51(6):1149–1168, 2017.

Michael Zimmer. “but the data is already public”: on the ethics of research in facebook. *Ethics and information technology*, 12(4):313–325, 2010.