RESEARCH · RESEARCH INTEGRITY

Research Ethics in Digital and Online Environments

The ethical questions raised by research using online platforms, social media and digital trace data, including whether public posts are fair game, consent at scale, re-identification risks, platform experiments, data protection law and practical guidelines.

ModQu research article · 1,576 words · 16 references (APA 7th edition)

The internet has opened vast new sources of data about human behaviour. Social media posts, online forums, search queries, purchase records and app usage all leave traces that researchers can analyse. Online surveys and experiments reach thousands of people at low cost. These opportunities raise ethical questions that traditional rules, written for laboratory experiments and face-to-face interviews, did not anticipate. This article sets out the main issues and the guidance that has developed to address them.

Why digital research is different

Several features of online research challenge established ethical practice.

Scale. A study may involve millions of people, making individual consent impractical.

Blurred boundaries between public and private. Material may be technically accessible to anyone, but posted by people who regard it as private or who did not imagine it being studied.

Persistence and searchability. Online content is stored indefinitely and can be searched, so quotations and data can be traced back to their authors.

Platform control. Much data is held by companies whose terms of service, rather than research ethics, govern its use.

Unclear research status. Analysis of existing digital data may not fit traditional definitions of research with human participants, and so may escape ethics review altogether. Metcalf and Crawford (2016) argued that this creates an ethics divide, in which some of the most consequential research on people receives the least oversight.

Is public data fair game?

A common assumption is that anything posted publicly may be used freely. Ethicists have challenged this. Eysenbach and Till (2001) argued that whether an online community should be treated as public or private depends on how its members perceive it, how many people take part, how easy it is to join and how sensitive the topic is. A support forum for people with a serious illness may be technically open, yet its members may reasonably expect not to be studied without being asked.

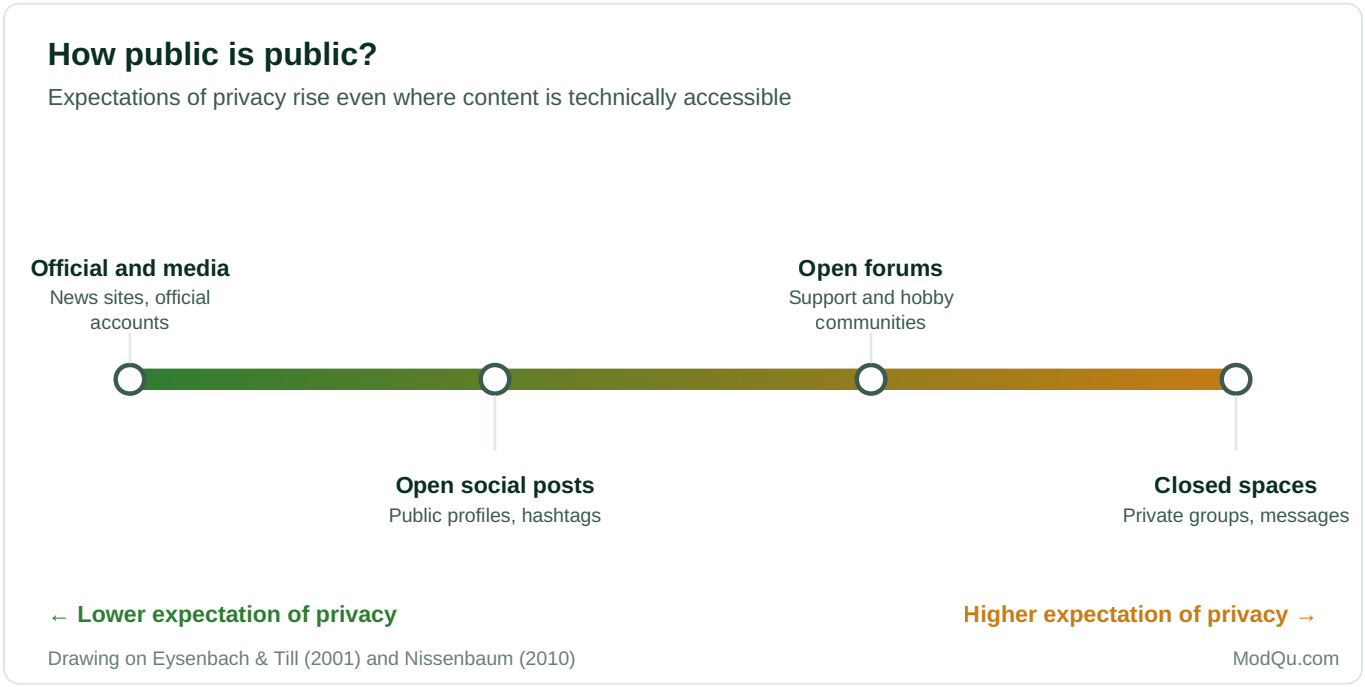


Figure 1. Online spaces differ in how far people expect privacy, regardless of technical access. Diagram by ModQu, drawing on Eysenbach and Till (2001) and Nissenbaum (2010).

Users' own views support this caution. Fiesler and Proferes (2018) surveyed Twitter users and found that most did not know their public posts could be used in research, and that their comfort depended on the context, such as who the researcher was and what the study was about. Williams et al. (2017) found that many users expected to be asked for consent before their posts were quoted in research publications, and to be anonymised.

Nissenbaum (2010) offered a useful framework, **contextual integrity**: information flows carry norms tied to the context in which they occur. Information shared among friends on a social platform carries different expectations from information published in a newspaper. Moving it into a new context, such as a research paper, may violate those norms even if the information was never secret.

Re-identification

Removing names does not make data anonymous. Sweeney (2002) showed that a few attributes, such as postcode, date of birth and sex, can uniquely identify most people when linked with other data sources. Narayanan and Shmatikov (2008) re-identified users in a supposedly anonymous data set of film ratings released for a public competition, by matching it with ratings people had posted publicly elsewhere. Rocher et al. (2019) estimated that almost all Americans could be correctly re-identified in an anonymised data set using a modest number of demographic attributes.

Zimmer (2010) described a research data set drawn from the social media profiles of a cohort of university students. Although the researchers removed names, the institution was quickly identified from published details, putting the students' privacy at risk.

Quotations create a specific risk. Ayers et al. (2018) found that, in a large share of health studies that quoted social media posts, the quoted text could be entered into a search engine to find the original post and its author. Even paraphrased quotations can sometimes be traced.

Experiments on platforms

Online platforms routinely test changes on their users. When such tests are designed to produce research findings, they raise questions about consent. Kramer et al. (2014) altered the emotional content of the news feeds of nearly 700,000 Facebook users to study whether emotions spread through social networks, relying on the platform's general terms of service as consent. The study prompted widespread criticism. Hallinan et al. (2020) analysed public reaction and found that many people objected to being manipulated without their knowledge, and were troubled by the gap between what they expected of the platform and what it did.

Covert observation and deception online

Online settings make it easy to observe without being seen. A researcher can join a forum, follow a group or create an account without revealing their purpose. Covert observation is not always wrong: it may be the only way to study some behaviour, such as the activities of extremist groups, and the risks to individuals may be low if results are reported carefully. But it removes participants' ability to decide whether to take part, so it needs strong justification. Guidance generally asks researchers to consider whether the research could be done openly, whether the knowledge gained justifies the deception, and how identities will be protected in publication. Creating fake profiles or interacting with users under false pretences raises further concerns and may also breach platform rules.

Vulnerable groups and sensitive topics

Many online communities exist precisely because their members share a sensitive experience: illness, addiction, bereavement, sexuality, migration status or involvement in crime. These communities are often valuable sources of insight, but their members may face real harm if exposed. Young people are another concern, since age is often unknown

online and children may be included in data without anyone realising. Research involving such groups calls for extra care: seeking permission from community moderators or members, avoiding direct quotation, and asking whether the study could cause distress or harm if members discovered it.

Researcher safety

Digital research can also expose researchers to risk. Those studying harassment, extremism or abuse may encounter disturbing material repeatedly, and those who publish on contentious topics may be targeted online. Research teams should plan for these risks, for example by limiting exposure to harmful content, offering support, and taking care with the personal information researchers make public.

Data protection law

In many jurisdictions, digital research must comply with data protection law. In the European Union, the General Data Protection Regulation applies to any processing of personal data, including data drawn from public sources, and treats pseudonymised data as personal data (Regulation (EU) 2016/679, 2016). It allows some flexibility for research, subject to safeguards such as data minimisation. Researchers working across borders need to understand the requirements in each relevant jurisdiction, as well as platform terms of service.

Guidelines and principles

The Association of Internet Researchers has developed widely used guidance. Its most recent version (franzke et al., 2020) rejects a single set of rules in favour of case-based reasoning, asking researchers to consider at every stage the context, the expectations of the people involved, the vulnerability of those affected and the potential for harm. Salganik (2018) proposed applying four principles to digital social research: respect for persons, beneficence, justice and respect for law and public interest, the last emphasising transparency and accountability. boyd and Crawford (2012) cautioned that big data does not speak for itself and that its use raises questions of access, power and responsibility that researchers must confront.

Practical steps

Researchers working with online data can follow several practical steps, summarised below.

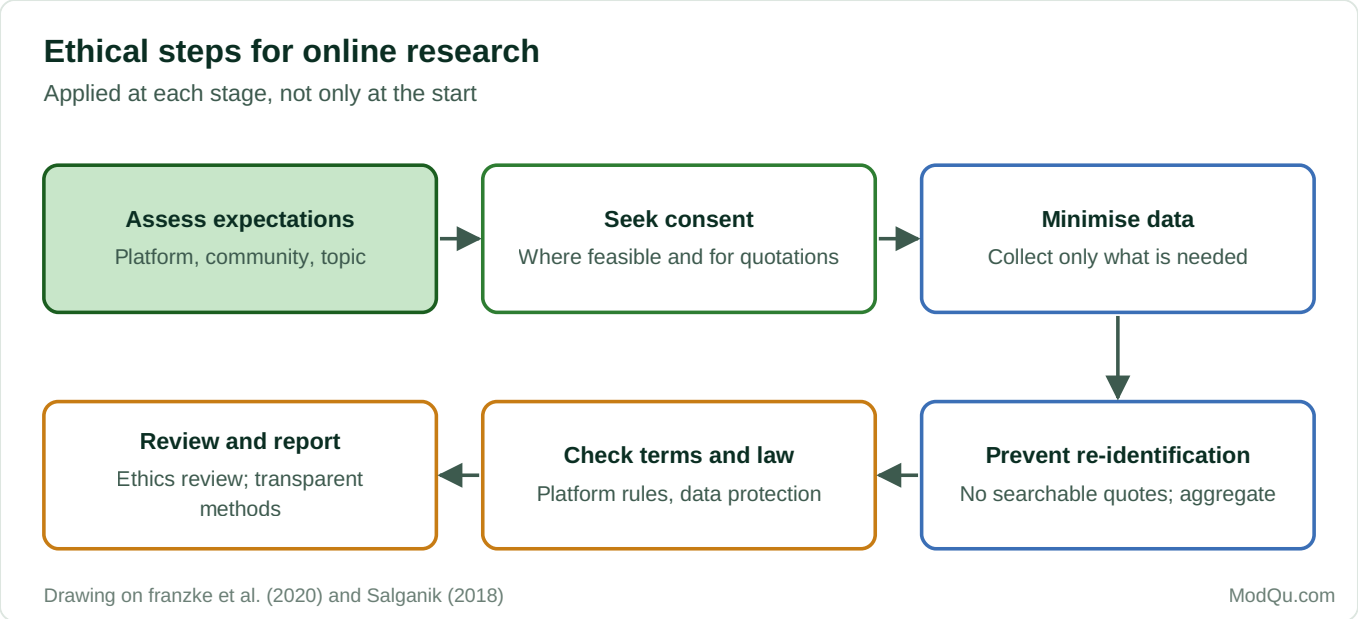


Figure 2. Practical steps for ethical research with online data. Diagram by ModQu, drawing on franzke et al. (2020) and Salganik (2018).

- **Assess expectations.** Ask how the people who created the data would view its use in research, considering the platform, community and topic.
- **Seek consent where feasible.** For small communities, sensitive topics and direct quotation, ask permission or notify participants.
- **Minimise data.** Collect only what the research question needs, and avoid storing identifying details.
- **Protect against re-identification.** Avoid verbatim quotations that can be searched, or alter them with care; aggregate results; limit access to raw data.
- **Respect terms and law.** Check platform terms of service and data protection requirements.
- **Seek review.** Submit digital research to ethics review even when it is not strictly required.
- **Be transparent.** Explain in publications how data were obtained and protected.

Implications for online surveys and business research

Online surveys and panels raise their own questions: how clearly participants are told what their data will be used for, whether incentives are fair, how data from devices such as location are handled, and how long responses are kept. In commercial settings, the line between research and marketing must be clear; people who agree to take part in research should not later find their answers used to target them with sales messages. Professional codes in market research require this separation and require that data be used only for the purposes participants agreed to.

Conclusion

Digital research offers unprecedented access to human behaviour, but the ease of collecting data does not settle whether it is right to use it. Public is not the same as fair game; removing names is not the same as anonymity; platform terms are not the same as informed consent. Contextual judgement, guided by principles of respect, beneficence, justice and accountability, and supported by practical safeguards, allows researchers to use online data while respecting the people who created it.

References

Ayers, J. W., Caputi, T. L., Nebeker, C., & Dredze, M. (2018). Don't quote me: Reverse identification of research participants in social media studies. *npj Digital Medicine, 1*, Article 30. https://doi.org/10.1038/s41746-018-0036-2

boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society, 15*(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *BMJ, 323*(7321), 1103–1105. https://doi.org/10.1136/bmj.323.7321.1103

Fiesler, C., & Proferes, N. (2018). "Participant" perceptions of Twitter research ethics. *Social Media + Society, 4*(1). https://doi.org/10.1177/2056305118763366

franzke, a. s., Bechmann, A., Zimmer, M., Ess, C., & the Association of Internet Researchers. (2020). *Internet research: Ethical guidelines 3.0*. Association of Internet Researchers. https://aoir.org/reports/ethics3.pdf

Hallinan, B., Brubaker, J. R., & Fiesler, C. (2020). Unexpected expectations: Public reaction to the Facebook emotional contagion study. *New Media & Society, 22*(6), 1076–1094. https://doi.org/10.1177/1461444819876944

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788–8790. https://doi.org/10.1073/pnas.1320040111

Metcalf, J., & Crawford, K. (2016). Where are human subjects in Big Data research? The emerging ethics divide. *Big Data & Society, 3*(1). https://doi.org/10.1177/2053951716650211

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy* (pp. 111–125). IEEE. https://doi.org/10.1109/SP.2008.33

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Regulation (EU) 2016/679. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88.

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications, 10*, Article 3069. https://doi.org/10.1038/s41467-019-10933-3

Salganik, M. J. (2018). *Bit by bit: Social research in the digital age*. Princeton University Press.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), 557–570. https://doi.org/10.1142/S0218488502001648

Williams, M. L., Burnap, P., & Sloan, L. (2017). 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. https://doi.org/10.1177/0038038517708140

Zimmer, M. (2010). "But the data is already public": On the ethics of research in Facebook. *Ethics and Information Technology, 12*(4), 313–325. https://doi.org/10.1007/s10676-010-9227-5