

COMMENTARY

Recommendations for conducting ethical network research

Francisca Ortiz Ruiz¹, Paola Tubaro², José Luis Molina³, Jennifer Watling Neal⁴,
Raffaele Vacca⁵, Jana Diesner⁶, jimi adams⁷, Michelle Birkett⁸, Jenny Godley⁹,
Juniper Lovato¹⁰, Michael Schönhuth¹¹, Laura Teves¹² and Michael Zimmer¹³

¹Centre for Economics and Social Policy, and School of Government and Public Administration, Universidad Mayor, Santiago, Chile and Millennium Institute for Care Research (MICARE), Santiago, Chile, ²Centre of Research in Economics and Statistics (CREST), CNRS-ENSAE-Polytechnic Institute of Paris, Palaiseau, France, ³GRAFO, Department of Social and Cultural Anthropology, Universitat Autònoma de Barcelona, Barcelona, Spain, ⁴Michigan State University, Michigan, USA, ⁵Department of Social and Political Sciences, University of Milan, Milan, Italy, ⁶Technical University of Munich and Munich Center for Machine Learning, Munich, Germany, ⁷University of South Carolina, USA, ⁸Center for Computational and Social Sciences in Health, and Department of Medical Social Sciences, Feinberg School of Medicine, Northwestern University, Chicago, IL, Chicago, USA, ⁹Department of Anthropology and Archaeology, University of Calgary, Canada, ¹⁰Computer Science, Vermont Complex Systems Institute, University of Vermont, Vermont, USA, ¹¹Department of Sociology/Anthropology, University of Trier, Trier, Germany, ¹²Universidad Nacional de la Plata, La Plata, Buenos Aires, Argentina, and ¹³Center for Data Ethics, Marquette University, USA

Corresponding author: José Luis Molina; Email: jose Luis.molina@uab.cat

Abstract

Ethical considerations in social network studies are grounded in the general principles of human subjects' research, including avoidance of harm, promotion of justice, equitable distribution of burdens and benefits, respect for human dignity, and protection of confidentiality. To help navigate these challenges, this article presents recommendations for conducting ethical network research, developed by a multi-disciplinary and multi-national working group. The article is divided in three main sections where there are certain recommendations identified for each one of them: data collections, use, and availability. Discovering how others addressed and solved problems can be a way for all of us to improve our capacity to stand up to the scrutiny of ethical governance bodies, while also increasing our capacity to responsibly address novel, rare, or otherwise difficult situations for which institutions provide limited guidance. We see this as a first step toward a virtuous circle, or a form of “generalized indirect reciprocity” whereby researchers share information that may be relevant for others, and benefit at the same time from the information given by other members of the social networks analysis community. Our goal is to continue to produce and promote scientifically solid, ethical social network research.

Keywords: Social network analysis; data collection; data use; data availability; ethical decisions; research ethics

1. Introduction

Ethical considerations in social network studies are grounded in the general principles of human subjects' research, including avoidance of harm, promotion of justice, equitable distribution of burdens and benefits, respect for human dignity, and protection of confidentiality. In this vein, Institutional Review Boards (IRBs—USA), Research Ethics Committees (RECs—Europe), Research Ethics Boards (REBs—Canada), and similar governance bodies elsewhere, expect network research practices to comply with sets of well-established rules and requirements. However, social network studies present challenges to meet even routine requirements such as confidentiality, as social network data offer more detailed information, and more ways to re-identify

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

individuals, than is usually the case (Hay *et al.*, 2010; Horawalavithana *et al.*, 2019). Because the details of ethical protocols and decisions are not commonly reported in scientific publications, much is left to network researchers' ability to negotiate their strategies individually and locally, resulting in very uneven outcomes. Indeed, many researchers in the field have experienced the frustration of having their ethical applications rejected, their fieldwork delayed, or their protocols distorted by the imposition of cumbersome additional procedures (Molina & Borgatti, 2021).

To help navigate these challenges, this article presents recommendations for conducting ethical network research, developed by a multi-disciplinary and multi-national working group. Table 1 in the Appendix summarizes these recommendations and can help as a memory-aid. Our main goal is to support researchers in their interactions with the ethical governance bodies of their institutions, providing documentation that they can refer to in order to properly justify their research design and the ethical choices that it implies. Thus, these recommendations are not to be seen as additional requirements that add to the burden of already heavy institutional processes, but rather as a tool to empower researchers when they negotiate with ethics committees, especially when the latter are very risk-averse or unfamiliar with social network analysis.

This article's practical purposes distinguish it from prior efforts to critically assess and reconceptualize ethical matters in social network research, as exemplified in the two special issues that the journal *Social Networks* devoted to this topic, respectively in 2005 (Breiger, 2005) and in 2021 (Tubaro *et al.*, 2021). Nor is this article a training tool like the network analysis manuals that increasingly offer ethical guidance, sometimes devoting entire chapters to it (Adams, 2019; McCarty *et al.*, 2019; Robins, 2015). Rather, the recommendations that we present below build on this literature to derive expectations, suggestions, and to some extent warnings. In this perspective, it follows the example of recent work that sets standards for reporting network data (Alieva *et al.*, 2026; Luke *et al.*, 2023) and for sharing such data (Neal *et al.*, 2024).

To work toward agreed recommendations, we took an end-to-end approach to ethics, considering every stage of the research process, from initial design to final delivery of results. We share the view of recent literature that demonstrates anonymity and consent are only part of a broader set of ethical complexities in social network research, despite their historical prominence and the challenges they continue to present. We identified three main domains of ethical concern within social network research: data collection, including issues related to informed consent and protection of confidentiality; data use, covering analysis, presentation of data and results, and visualization; and finally, data availability, an umbrella expression for publication, data storage, and data sharing. Concretely, we split into subgroups, one for each domain, in charge of reviewing related topics in recent literature and of drafting preliminary versions. Several cross-group meetings, both online and in-person at past Sunbelt conferences, enabled revisions based on mutual feedback and ultimately ensured consistency throughout the work. The outcome of this collective effort, organized by domain, is presented below.

To maximize the usefulness of these recommendations, we also prepared a shorter version of this document (<https://network-ethics.github.io/assets/images/ExecSummary.pdf>), with the idea that researchers can take it to their IRB (or REC, REB, etc., depending on their institutional context) as supporting evidence to their claim that they are meeting the standard ethical expectations of the social network analysis community. The present article is, instead, designed for researchers themselves, helping them with more detailed explanations and with references to the relevant literature.

These agreed recommendations take the view that even well-established principles are contingent and need to be adapted to context. For example, the encouragement to share data as much as possible comes with awareness that it is not advisable to do so when personally identifiable information is present (Neal *et al.*, 2024). Instead of imposing rigid principles or rules, consideration of contextual factors invites researchers to think reflectively and responsibly—as active contributors to, rather than passive adopters of, ethical research practices. This does not necessarily mean softening the standards that ethical governance bodies typically uphold. Quite in contrast, the below recommendations also alert researchers about issues that we are aware of as

network specialists, but that often escape institutions and others involved in the research process. For example, Chu et al. (2021) show that social media data may reveal health-related information about individuals in ways that are difficult to predict in advance. Overall, it is our view that the material reported below has potential to advance the capacity of the social network research community to act ethically, even beyond the confines of externally imposed governance systems.

2. Data collection: Consent and confidentiality protection

In line with the general principles of human subjects' research, IRBs, RECs and REBs routinely require a) informed consent from participants, signifying fully voluntary participation and allowing opt-out at any point without reprisal (Helsinki Declaration, 1964, article 4B), and b) confidentiality protection, whether in the form of complete and irreversible anonymization or of pseudonymization accompanied by complementary measures in terms of data security, access control, user training, and appropriate licensing. However, standard procedures for obtaining participant consent and for implementing anonymization or pseudonymization (see Kadushin, 2005; McCann, 2022; Pallotti, et al., 2022) present unique challenges in network research. First, non-participation can have consent implications for both participants strictly speaking (i.e., those who provide data about themselves, for example *egos* in personal network research) and non-participants (i.e., those whose data are reported by others in the network, for example *alters* in *ego*-network studies: see Lovato et al., 2022). Second, it is difficult to ensure consent, typically conceptualized and operationalized at individual level, with network data that entail two or more interdependent persons (i.e., members of a relationship). Third, anonymization and even pseudonymization are incompatible with many network research designs, at least at data collection stage, as names are essential to identify social ties.

As a general rule, network researchers should gain informed consent from participants. Consent may be written, electronic, or oral, depending on the circumstances, and in all cases along the lines of standard expectations for any research with human subjects. Further, three primary strategies are available to address consent implications for non-participants, drawing on practices from other fields. Of note, such strategies only pertain to situations where personally identifying information is provided about others, not where such information is gathered anonymously, in which case that information can likely be considered as not representing personal data. For example, in most *ego* network designs, these concerns can be assuaged by eliciting information about one's *alters* in anonymous (or pseudonymous) formats (Adams, 2019; McCarty et al., 2019; Perry et al., 2018).

Use two-stage consent for closed populations. When dealing with “closed” populations such as members of organizations, companies, or schools, you may consider getting consent from the entire population under study, *prior* to gathering any data. This first strategy pertains both to whether individuals consent to participating in the research themselves (e.g., as survey or interview respondents), and whether they consent to having information about them provided by others. These dimensions are potentially independent from each other. This two-stage consenting process can either take the form of passive (“opt-out”) or active (“opt-in”) consent, depending on the potential sensitivity and details of the information to be gathered. It can also be based on the requirements agreed upon if these closed populations represent organizations, as was done with the schools in the Add Health study (Bearman et al., 1997).

Treat *alters* as “secondary participants.” This second strategy recognizes that traditional consent procedures are oriented towards individual-level data and therefore do not apply in the same way to relational data. At the same time, it acknowledges the need to reduce any potential risks that might derive from unauthorized disclosure of personal data about secondary participants. Standards of data collection and protection for secondary participants have a long history in a variety of fields but have not always been recognized as aligning with the needs

of social network analysis. For example, in demographic research, a single representative of a household often provides (sometimes highly sensitive) information about other members of the household. There are a variety of principles drawn upon to justify this strategy as consistent with the *intents* of informed consent and data protection provisions in IRBs/RECs/REBs, if not directly replicating the standard procedures for their implementation. One such principle is considering the information that a respondent provides about others as their *perceptions* of that information, and therefore not a capture of these other people's data without their consent. This distinction has direct parallels to the difference between participants and informants, commonly adopted in communications research. This approach also draws from the principle (if not practice) of standard IRB/REC/REB orientations concerning the differentiation between information that can reasonably be assumed to be private, versus that which should be assumed to be known or knowable by others (a standard that is often weighed in considering the ethical approaches governing "collective consent" ideas in ethnographic research, from the Ethical Guidelines for good research practice, 2021, <https://theasa.org/ethics/>). That is, if others are providing information about an individual that is already publicly available in some non-private form, further sharing of that same information with researchers is not seen as violating standards of expected privacy. That said, none of these principles provide full justification for providing/gathering information about secondary participants without their consent. As such, each of these possibilities must be applied in conjunction with measures to ensure data protection and minimization of potential risks for secondary participants alongside primary participants. In some settings, secondary participants-based strategies still require IRB/REC/REB waivers of consent, but are appropriate, especially when entailing minimal risks and when research is impossible to conduct without the waiver of consent (see Klov Dahl, 2005).

Use chain referral with anonymized tokens. The third strategy is an adaptation of chain referral approaches, where respondents first provide linkable information about *alters* in an anonymized fashion, then recruit those nominated partners into the study in a way that allows the relational information to be linkable between the pairs of participants. This strategy has been used in Respondent Driven Sampling and other partner-recruitment designs through the distribution of anonymized unique numeric "tokens" (Hâncian et al., 2021).

All these strategies are ways to meet the expectation of free, informed and voluntary inclusion in a study, even in the case of non-participants who do not provide consent in traditional ways. Note, also, that some legal and ethical authorities accept personal data processing without consent in special cases. These may include, depending on the context, research that demonstrably serves the public interest and cases in which it is impossible to collect consent from all concerned persons, it may endanger vulnerable participants, or it may reduce the accuracy of the data to be collected. In these cases, researchers must still protect the data subjects, notably by informing subjects (and any other stakeholders) about their planned studies, establishing procedures to opt out, and implementing strict disclosure control measures. This is often achieved, at least in part, through anonymization or pseudonymization, which as discussed are difficult to apply to social network analysis. Therefore, we next turn to recommendations on how to adapt typical confidentiality requirements for network research.

Use pseudonymization (with acronyms) or delayed anonymization. When anonymous data collection is not possible, researchers may simply request and record acronyms or pseudonyms for both respondents and their contacts, provided that this does not lead to loss of any essential information. IRBs and RECs/REBs routinely approve this solution, which is suitable for many *ego* network designs. However, the acronym-based mitigation strategy is not suitable for complete or "partial" network designs in which data linkages between members of a study population are necessary. Additionally, and more generally, limitations of disambiguation (i.e., when identifiers are not sufficiently distinct) and accuracy (e.g., when ties can no longer be correctly linked to the parties involved in them) may compromise data analysis. Under these conditions, "delayed

anonymization” offers a valuable alternative, whereby researchers collect real names or other forms of personal identifying information, with steps to protect that data to follow later. It should be recognized in this respect that it might still be too early to anonymize or even pseudonymize network data at pre-processing stage (that is, *after* collection and *before* analysis). Depending on the research question and setting, it may sometimes be preferable to leave anonymization to the post-processing phase (*after* analysis and *before* presentation of results). Of course, working with non-anonymous data during the first phases of the research requires extra security measures, such as storage in a protected institutional repository, encryption, and controlled access. In the case of elicitation methods using digital trace data, the same principles apply.

Minimize data collection. Finally, and as a general rule, it is important to adhere to the principle of minimization when collecting personal information (on both participants and non-participants), limiting the data gathering to the strictly necessary required to achieve the research goals.

Recognize that consent and confidentiality are tightly coupled in network research. The preceding considerations highlight an important dimension of network data that differentiates it from “standard” human subjects research strategies. While IRBs (or RECs, REBs, etc.) often view informed consent and confidentiality protection as two essentially separate aspects, they are almost always intertwined in network data (see also Tubaro, 2021; Stys et al., 2022). For example, minimizing risks for non-participants who do not give their explicit consent requires strict controls to avoid any disclosure of potentially identifiable information.

Taken together, these considerations suggest that consent procedures in network research should be explicit about the relational nature of the data, proportionate to the risks involved, and transparent about how secondary participants are protected. Researchers are encouraged to document these procedures, including any justified waivers of individual consent, and to align confidentiality protections (such as data minimization, pseudonymization, and restricted access) with both regulatory requirements and participants’ expectations. Some of these elements carry over into data analysis, presentation, and use considerations, which are addressed in more detail in the following section.

3. Data use: Analysis, presentation, & visualization

The use of network data is a process that unfolds over time and across practices, rather than as a single technical operation. This process can be understood as moving from the analysis of data to the presentation of results through, first, text, tables, and non-network visual tools, and second, the visual representation of networks themselves. Decisions made at each stage shape the ethical and interpretive possibilities of the next, making it essential to consider them as part of a continuous narrative of research practice. Overall, eight main recommendations emerge.

Specify team roles and protect data throughout the analytical workflow. The analytical stage sets the tone for everything that follows. It is here that organizational choices, interpretive frameworks, and ethical commitments first take concrete form. A central concern at this stage is how research teams structure their collaboration. Data management plans should therefore specify the roles of all team members and clarify how they will work together across the lifecycle of the project. Beyond data collection, these arrangements influence the handling of raw, intermediate, and final datasets. Network analysts are not without guidance in this respect: a substantial body of literature offers insights into how teamwork can be organized in ways that respect existing ties while also harnessing their potential for effective collaboration (Pauksztat, 2022).

The obligation to protect data is an essential part of any data management plan. Analytical work often involves moving data across platforms, devices, and services, making it essential to remain aware of where data are stored and under what conditions they are processed. This includes

scrutinizing the terms of use of cloud-based tools to prevent unauthorized access or loss of control. In institutional contexts, additional safeguards are needed to ensure that personal network data are not repurposed for evaluation or surveillance, particularly when agreements with organizations are in place (Borgatti & Molina, 2005; Töpfer & Hollstein, 2021; Vorös *et al.*, 2021).

Document data provenance and preprocessing decisions. The credibility of any analysis also depends on its traceability. As results accumulate, so too does the need for careful documentation. Beyond general best practices for data documentation (Gebru *et al.*, 2021), network research requires explicit accounts of how nodes and ties were defined, constructed, and bounded in time and space. References to data sources, platforms, or providers should be included wherever relevant. Making these decisions visible—whether in main texts, supplementary materials, or formats such as network cards—ensures that analytical claims remain interpretable and contestable (Bagrow & Ahn, 2022).

Be transparent about funding sources. Questions of accountability extend beyond data handling to the broader political and institutional environment of research. As network analysis increasingly attracts interest from governmental and corporate actors, transparency about funding sources and external involvement becomes indispensable. Fully disclosing the roles and interests of non-academic funders allows readers and participants alike to assess potential conflicts and anticipate downstream uses of the research.

Avoid deterministic interpretations and value diversity without stigmatizing groups. From these organizational foundations, attention must turn to interpretation. Analytical results do not exist in a vacuum; they interact with the meanings that participants themselves attach to their social relationships. As in other areas of the social sciences, researchers' conceptual categories may diverge from participants' lived understandings of their social worlds. Network measures such as centrality or cohesion capture structural properties, but they do not necessarily reflect how relationships are experienced, narrated, or valued by those involved. Interpreting participants' accounts therefore requires caution, particularly since people may frame their narratives through an awareness of contemporary networking discourses that only partially overlap with analytical tools (D'Angelo & Ryan, 2021).

These interpretive limits become especially visible when considering the scope of inference. Even when network datasets appear comprehensive, they are usually embedded in specific organizational, institutional, or local contexts. Rarely are they derived from representative population samples. For this reason, network analyses often function more like case studies than like generalizable surveys, and their findings must be interpreted accordingly (Crossley & Edwards, 2016). The same caution applies to common explanatory mechanisms. While homophily and social influence are well-established mechanisms that operate in social networks, they do not do so in deterministic ways. Network proximity does not imply uniformity of values, preferences, or behaviors, and analysts should resist interpretations that reduce individual agencies to network position alone.

As interpretation moves from individuals to groups, another layer of responsibility emerges. Network methods are particularly well suited to revealing diversity, clustering, and differentiation within social structures. Community detection techniques and exploratory visualizations of attributes can illuminate how groups form and interact and may even inform targeted interventions or policy design. Yet these same strengths carry risks. When findings are removed from their analytical context, they may be appropriated or misread by non-specialist audiences, reinforcing stereotypes or discriminatory narratives—especially about marginalized populations. For instance, evidence of ethnic homophily in immigrant networks may be misconstrued as deliberate social withdrawal rather than as a context-dependent pattern of interaction. Anticipating such misinterpretations, and adopting strategies to mitigate harm, is therefore a critical part of ethical analysis (Bright *et al.*, 2021).

Ensure nodes remain non-identifiable in all outputs. As analysis gives way to presentation and visualization, earlier decisions continue to resonate. A core principle links these later stages: the protection of participants' personal data. Even when identifiers are removed, small or well-known networks may allow re-identification through combinations of attributes and structural positions. For this reason, confidentiality measures must accompany not only analysis, but also the ways results are written, tabulated, and displayed. Network-specific strategies for presentation and visualization can reduce these risks, if they are explicitly documented and carefully adapted to context. The following recommendations detail these aspects further.

Present results to participants when feasible. At this point in the research process, the analytical stage opens outward toward those who are being studied—participants, their community, and any other stakeholders. Involving community members—where feasible—can enrich analysis and foster reciprocity. Such involvement may take modest forms, such as acknowledgment or data access, or more substantial ones, such as collaboration or co-authorship (Carroll et al., 2020; Tubaro, 2021). Yet engagement also entails uncertainty, particularly when results are taken up in ways researchers cannot fully control. These possibilities must be weighed carefully, with attention to context and potential consequences.

In particular, presentation creates opportunities for dialogue. When context and anonymization permit, sharing results with participants can serve as a form of validation and reflexive correction, particularly if undertaken before analyses are finalized. It may also extend the impact of research beyond academic audiences. Because such feedback loops can influence expectations and experiences, they should be anticipated and addressed in consent procedures from the outset (Tubaro, 2021). Likewise, visualizations may return the research process to participants and communities. For some, seeing a representation of their own network can be affirming or even therapeutic, and has been used in care and rehabilitation contexts (Hogan, et al., 2007; Nicaise et al., 2022). For others, however, such images may provoke discomfort by making isolation or vulnerability visible (D'Angelo & Ryan, 2021). Navigating this tension requires attention to context and, where necessary, provision of support and advice. When carefully managed, network visualizations can do more than display results: they can invite reflection, elicit feedback, and generate new narratives that deepen understanding of social connections (Molina et al., 2014).

Make visualizations transparent and accessible. Researchers should pay attention to how visualization choices can highlight certain dimensions while downplaying others, making transparency essential. Researchers should clearly report the tools, models, measures, software, and parameters used to generate visual outputs, for example through supplementary materials or network cards (Bagrow & Ahn, 2022). Accessibility is also part of responsible visualization, using clear legends, captions, color-blind-friendly palettes, and alternative text descriptions.

Exercise caution when sharing results on social media. While dissemination of research findings increasingly takes place in networked public spaces online, the speed and reach of these platforms heighten the risks associated with sharing sensitive material. Researchers must therefore exercise particular care to ensure that posts, images, or summaries do not inadvertently expose private information.

4. Data availability: Data storage, publication, and sharing

The ethical principles governing data protection extend across all forms of research dissemination, including publications, oral presentations, and posters. In each of these contexts, researchers should avoid labels, descriptions, or contextual details that could enable personal identification even indirectly (Tubaro et al., 2021). Where appropriate, individuals involved in the research may be invited to provide feedback on specific excerpts of the material to be published, particularly when these include interview transcriptions or network visualizations that represent their relationships (Tubaro, 2021). A few main recommendations emerge.

Use secure institutional repositories when possible. Throughout the research data lifecycle, researchers are expected to comply with governmental and institutional regulations, as well as with disciplinary norms and publisher guidelines when applicable. Along these lines, they should store and manage data within secure institutional repositories (Neal *et al.*, 2024) wherever possible. Importantly, these frameworks are not static: requirements related to issues such as terms of service or web scraping conditions may evolve over time and differ across jurisdictions.

Store identifiers separately in access-restricted folders. In cases where data are pseudonymized, but not fully anonymized, any personal identifiers should be stored separately in access-restricted folders available only to authorized personnel, in order to minimize the risk of re-identification.

Replace identifiers with codes, aggregate variables, reduce granularity; apply k-anonymity or differential privacy when appropriate; exercise extra care for case studies and small samples.

To ensure safe publication of a dataset, further steps should be taken to anonymize the data: identifiable information may be replaced with codes, variables may be aggregated, data granularity reduced, and broader geographic markers employed, among other techniques (Alieva *et al.*, 2026). In some cases, disclosure control measures beyond de-identification and basic pseudonymization may be required even before data are shared internally within a research team. Additional safeguards, such as k-anonymity or differential privacy, can further strengthen protection. These provisions are particularly important when data sharing may inadvertently cause harm, reinforce stereotypes, or generate discriminatory interpretations, especially toward already marginalized groups. Because relational data can reveal identities indirectly—through contextual descriptions, shared demographic characteristics, or the visibility of network ties—extra care is required at the anonymization stage, particularly with in-depth case studies and small-samples.

Share data via repositories (GitHub, OSF) when feasible; provide curated subsets if full sharing is not possible; plan sharing strategies from project outset; balance transparency with privacy protection. Neal *et al.* (2024) encourage network researchers to share anonymized or (where additional safeguards are in place) pseudonymized data through recognized online repositories such as GitHub or the Open Science Framework (OSF). In some contexts, making these repositories accessible and meaningful to participants themselves (and/or other stakeholders) may also be appropriate, although this decision should be guided by context-specific considerations. When full data sharing is not possible, authors may instead provide a curated subset of the data or create an openly accessible project page on OSF (Pasquale *et al.*, 2025). Planning data-sharing strategies from the outset of a project can enhance transparency, replicability, and accountability, both within the scientific community and toward the broader environment of the research, also including participants. In studies of online networks, data sharing can further support the validation of findings and facilitate comparison across research settings. For this reason, researchers should consider potential data-release strategies early in the research process and clearly communicate these plans to participants in advance.

5. Final reflections

The above considerations reveal that the social network research community has made significant progress since researchers and ethics boards first raised ethical concerns about anonymity and consent in social network research. These two issues remain emblematic of the specific challenges that arise with network data, if only because they are more tightly coupled to each other than in other fields. Nevertheless, the section on “Data collection” presented earlier also highlights that multiple solutions to both types of issues have already been attempted and may inspire the work of future researchers. While each scholar will have to identify which solutions best suit a specific study setting, they together demonstrate that these problems are not unsolvable and that there are many ways of conducting network studies that meet even very high ethical expectations.

The section on “Data use” moves beyond the data collection stage to consider the analysis of data and its presentation to the public, either through visualizations or in any other way (for example, text or tables). Because all these activities may generate impacts on various individuals and/or groups, they inherently raise ethical questions and require suitable answers. For this reason, the Data use section contains multiple recommendations, many of which can enhance the capacity of the network research community to stick to high ethical standards. Examples include transparency about funding sources, systematic data documentation, and measures to ensure personal data protection—potentially including a clear division of roles within a research team. Other recommendations may even advance our ethical stance well beyond typical institutional requirements. For example, using field-specific insights about the meanings that respondents may give to their relationships and networks, and how they may differ from the outputs of our measures and models, is a dimension that few institutional bodies can anticipate, but that can bring us a long way towards appropriate recognition of the possible impacts of our research, and toward adoption of mitigating strategies if necessary. Likewise, the recommendations of exercising caution before generalizing results or sharing them on social media, of fostering the involvement of participants and stakeholder communities where possible, and of thoroughly explaining visualizations, draw from our scientific knowledge and at the same time strengthen our capacity to maximize the societal benefits of our research.

The section on “Data availability” stretches ethical considerations to the last phases of research, including an explicit consideration for the sharing of results and data. Following Neal et al. (2024), we see the sharing of data (and, where relevant, code, procedures, etc.) as good practice, though the challenge is to find the right balance between the desire for openness and the need to continue protecting personal data.

With this analysis, we have put into practice the suggestion of Tubaro et al. (2021) that the social network analysis community works at its best when collectively addressing ethical dilemmas. The recommendations we outlined derive from our own experiences and from our reading of existing literature, and they are intended to benefit all researchers in the field. Discovering how others addressed and solved problems can be a way for all of us to improve our capacity to stand up to the scrutiny of ethical governance bodies, while also increasing our capacity to responsibly address novel, rare, or otherwise difficult situations for which institutions provide limited guidance. We see this as a first step toward a virtuous circle, or a form of “generalized indirect reciprocity” whereby researchers share information that may be relevant for others, and benefit at the same time from the information given by other members of the social networks analysis community. Our goal is to continue to produce and promote scientifically solid, ethical social network research.

Acknowledgments. We would like to acknowledge members of the International Network for Social Network Analysis (INSNA) for feedback on early versions of this paper.

Competing interest. None

Funding statement. None

Data availability statement. There is no data used during the article, therefore it is not available.

References

- Adams, J. (2019). *Gathering Social Network Data*. Thousand Oaks: SAGE. <https://doi.org/10.4135/9781544321486>.
- Alieva, D., Erices Ocampo, P., Ortiz Ruiz, F., Romero Mendoza, V., Salej Higgins, S., Tubaro, P., & Maya Jariago, I. (2026). Guidelines for reporting social and personal network data: The case of the journal REDES. *Redes. Revista Hispana Para El análisis De Redes Sociales*, 37(1), 1–15. <https://doi.org/10.5565/rev/redes.1122>.
- Bagrow, J., & Ahn, Y. Y. (2022). Network cards: concise, readable summaries of network data. *Applied Network Science*, 7(1), 84. <https://doi.org/10.1007/s41109-022-00514-7>.
- Bearman, P. S., Jones, J., & Udry, J. R. (1997). *The National Longitudinal Study of Adolescent Health: Research Design*. Chapel Hill, NC: Carolina Population Center.

- Borgatti, S. P., & Molina, J. L. (2005). Toward ethical guidelines for network research in organizations. *Social Networks*, 27(2), 107–117. <https://doi.org/10.1016/j.socnet.2005.01.004>.
- Breiger, R. (2005). Introduction to special issue: Ethical dilemmas in social network research. *Social Networks*, 27(2), 89–93. <https://doi.org/10.1016/j.socnet.2005.01.002>.
- Bright, D., Brewer, R., & Morselli, C. (2021). Using social network analysis to study crime: Navigating the challenges of criminal justice records. *Social Networks*, 66, 50–64. <https://doi.org/10.1016/j.socnet.2021.01.006>.
- Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). The CARE principles for indigenous data governance. *Data Science Journal*, 19(1), 1–12. <https://doi.org/10.5334/DSJ-2020-043>.
- Chu, K. H., Colditz, J., Sidani, J., Zimmer, M., & Primack, B. (2021). Re-evaluating standards of human subjects protection for sensitive health data in social media networks. *Social Networks*, 67, 41–46. <https://doi.org/10.1016/j.socnet.2019.10.010>.
- Crossley, N., & Edwards, G. (2016). Cases, mechanisms and the real: The theory and methodology of mixed-method social network analysis. *Sociological Research Online*, 21(2), 217–285. <https://doi.org/10.5153/sro.3920>.
- D'Angelo, A., & Ryan, L. (2021). The presentation of the networked self: Ethics and epistemology in social network analysis. *Social Networks*, 67, 20–28. <https://doi.org/10.1016/j.socnet.2019.06.002>.
- Geburu, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Iii, H. D., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, 64(12), 86–92.
- Hâncean, M.-G., Lubbers, M. J., & Molina, J. L. (2021). Measuring transnational social fields through binational link-tracing sampling. *PLoS One*, 16(6), e0253042. <https://doi.org/10.1371/journal.pone.0253042>.
- Hay, M., Miklau, G., Jensen, D., Towsley, D., & Li, C. (2010). Resisting structural re-identification in anonymized social networks. *The VLDB Journal*, 19(6), 797–823.
- Hogan, B., Carrasco, J. A., & Wellman, B. (2007). Visualizing personal networks: Working with participant-aided sociograms. *Field Methods*, 19(2), 116–144. <https://doi.org/10.1177/1525822X062985>.
- Horawalavithana, S., Arroyo Flores, J., Skvoretz, J., & Iamnitchi, A. (2019). The risk of node re-identification in labeled social graphs. *Applied Network Science*, 4(1), 33.
- Kadushin, C. (2005). Who benefits from network analysis: Ethics of social network research. *Social Networks*, 27, 139–153.
- Klovdahl, A. S. (2005). Social network research and human subjects protection: Towards more effective infectious disease control. *Social Networks*, 27(2), 119–137.
- Lovato, J. L., Allard, A., Harp, R., Onaolapo, J., & Hébert-Dufresne, L. (2022). Limits of individual consent and models of distributed consent in online social networks. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 2251–2262.
- Luke, D. A., Tsai, E., Carothers, B. J., Malone, S., Prusaczyk, B., Combs, T. B., Vogel, M. T., Neal, J. W., Neal, Z. P., & Ghinoi, S. (2023). Introducing soNHR—reporting guidelines for social networks in health research. *PLoS one*, 18(12), e0285236. <https://doi.org/10.1371/journal.pone.0285236>.
- McCann, M. (2022). Working paper: Guidance on processing data on interpersonal relationships for social network research. MRC/CSO Social and Public Health Science Unit: University of Glasgow.
- McCarty, C., Lubbers, M. J., Vacca, R., & Molina, J. L. (2019). *Conducting Personal Network Research: A Practical Guide*. New York: Guilford Publishers.
- Molina, J. L., Maya-Jariego, I., & McCarty, C. (2014). Giving meaning to social networks: Methodology for conducting and analyzing interviews based on personal network visualizations. In Domínguez, S., & Hollstein, B. (eds.), *Mixed Methods in Social Network Research. Design and Applications*. Cambridge: Cambridge University Press. pp. 305–335.
- Molina, J. L., & Borgatti, S. P. (2021). Moral bureaucracies and social network research. *Social Networks*, 67, 13–19. <https://doi.org/10.1016/j.socnet.2019.11.001>.
- Neal, Z. P., Almquist, Z. W., Bagrow, J., Clauset, A., Diesner, J., Lazega, E., Lovato, J., Moody, J., Peixoto, T. P., Steinert-Threlkeld, Z., & Teixeira, A. S. (2024). Recommendations for sharing network data and materials. *Network Science*, 12(4), 404–417. <https://doi.org/10.1017/nws.2024.16>.
- Nicaise, P., Garin, H., Smith, P., d'Oreye de Lantremange, S., Leleux, L., Wyngaerden, F., & Lorant, V. (2022). Implementation of a computer-assisted face-to-face intervention for mapping the social support networks of patients with severe mental illness in routine clinical practice: Analysis of the appropriateness and acceptability of the intervention. *International Journal of Social Psychiatry*, 68(8), 1774–1782. <https://doi.org/10.1177/0020764021105897>.
- Pallotti, F., Weldon, S. M., & Lomi, A. (2022). Lost in translation: Collecting and coding data on social relations from audio-visual recordings. *Social Networks*, 69, 102–112. <https://doi.org/10.1016/j.socnet.2020.02.006>.
- Pasquale D. K., Wolff, T., Varela, G., Adams, J., Mucha, P. J., Perry, B. L., et al. (2025). Considerations for social networks and health data sharing: An overview. *Annals of Epidemiology*, 102, 28–35. <https://doi.org/10.1016/j.annepidem.2024.12.014>.
- Pauksztat, B. (2022). Social networks and resilience in work teams. In Lazega, E., Snijders, T. A. B., & Wittek, R. (eds.), *A Research Agenda for Social Networks and Social Resilience*. Cheltenham: Edward Elgar. pp. 31–44. <https://doi.org/10.4337/9781803925783.00008>.
- Perry, B. L., Pescosolido, B. A., & Borgatti, S. P. (2018). *Egocentric Network Analysis: Foundations, Methods, and Models*. Cambridge, MA: Cambridge University Press. <https://doi.org/10.1017/9781316443255>.
- Robins, G. (2015). *Doing Social Network Research. Network-based Research Design for Social Scientists*. Thousand Oaks: SAGE.

- Stys, P., Muhindo, S., N'simire, S., Tchumisi, I., Muzuri, P., Balume, B., & Koskinen, J. (2022). Trust, quality, and the network collection experience: A tale of two studies on the Democratic Republic of Congo. *Social Networks*, 68, 237–255. <https://doi.org/10.1016/j.socnet.2021.08.002>.
- Töpfer, T., & Hollstein, B. (2021). Order of recall and meaning of closeness in collecting affective network data. *Social Networks*, 65, 124–140. <https://doi.org/10.1016/j.socnet.2020.12.006>.
- Tubaro, P., Ryan, L., Casilli, A. A., & D'Angelo, A. (2021). Social network analysis: New ethical approaches through collective reflexivity. *Social Networks*, 67, 1–8. <https://www.sciencedirect.com/science/article/pii/S0378873320301003>.
- Tubaro, P. (2021). Whose results are these anyway? Reciprocity and the ethics of “giving back” after social network research. *Social Networks*, 67, 65–73. <https://doi.org/10.1016/j.socnet.2019.10.003>.
- Vörös, A., Boda, Z., Elmer, T., Hoffman, M., Mephram, K., Raabe, I. J., & Stadtfeld, C. (2021). The Swiss student Life study: Investigating the emergence of an undergraduate community through dynamic, multidimensional social network data. *Social Networks*, 65, 71–84. <https://doi.org/10.1016/j.socnet.2020.11.006>.

Appendix

Table A1. Recommendations

Data collection	Consent & personal data
Consent strategies	<ul style="list-style-type: none"> • Use two-stage consent for closed populations • Treat alters as “secondary participants” • Use chain referral with anonymized tokens
Confidentiality protection	<ul style="list-style-type: none"> • Recognize that consent and confidentiality are tightly coupled in network research • Use pseudonymization (with acronyms) or delayed anonymization • Minimize data collection
Data use	Analysis, presentation, & visualization
Analysis	<ul style="list-style-type: none"> • Specify team roles & protect data throughout analytical workflow • Document data provenance and preprocessing decisions • Be transparent about funding sources • Avoid deterministic interpretations; value diversity without stigmatizing groups
Presentation & visualization	<ul style="list-style-type: none"> • Ensure nodes remain non-identifiable in all outputs • Present results to participants when feasible • Make visualizations transparent and accessible • Exercise caution when sharing on social media
Data availability	Storage, publication, & sharing
Storage	<ul style="list-style-type: none"> • Use secure institutional repositories when possible • Store identifiers separately in access-restricted folders
Publication	<ul style="list-style-type: none"> • Replace identifiers with codes, aggregate variables, reduce granularity • Apply k-anonymity or differential privacy when appropriate • Exercise extra care for case studies and small samples
Sharing	<ul style="list-style-type: none"> • Share via repositories (GitHub, OSF) when feasible • Provide curated subsets if full sharing is not possible • Plan sharing strategies from project outset • Balance transparency with privacy protection

Cite this article: Ortiz Ruiz F., Tubaro P., Molina J. L., Neal J. W., Vacca R., Diesner J., Adams J., Birkett M., Godley J., Lovato J., Schönthuth M., Teves L. and Zimmer M. (2026). Recommendations for conducting ethical network research. *Network Science* 14, 1–11. <https://doi.org/10.1017/nws.2026.10034>