1 Ethics in networks

These notes are not a complete or even a thorough exploration of ethics and networks. The topic is too broad and dynamic to cover entirely. Rather, these notes are meant to highlight four categories of ethical questions that arise in network data, and to surface specific points for consideration and discussion.

The big picture. Network data inherits all the ethical considerations that go along with any other type of empirical data. But, they also pose additional ethical complexities because network data—the edges—are explicitly non-independent with respect to the nodes: if we add or remove an edge, we may change all manner of other characteristics of the network. This non-independence implies that information about one node provides information about other nodes, and ethical concerns cannot be isolated down to single nodes independently.

1.1 Ethics and measurement

Measuring a network, i.e., recording social interactions among people, is an act of power—a power to see the social environment in which these individuals are embedded, and to reveal information, which some individuals may prefer to remain hidden (to protect themselves, or an advantage), or which may benefit all or just some. By measuring and recording the interactions in a network form, localized information is made global, persistent, shareable, and analyzable.

Networks that relate to people raise fairly clear ethical concerns, even in the very act of measuring them. For instance, sexual networks, where nodes are people and edges represent sexual interactions, can be useful for studying the spread of disease. But assembling such a network typically requires asking individuals to share a list of their sexual partners with you, a researcher, and potentially whomever later has access to the data, which poses privacy risks to the individuals and to their partners. Examples of sensitive social network information abound: criminal, secret or just clandestine interactions, economic transactions,[1] mobile phone calls, medical interactions, and many more. In fact, even deciding which types of interactions to record (and which to ignore) can be sensitive.

Other networks may seem ethically free because of their subject matter. Species in a food web have no expectation of privacy, and don't care about being represented in a network. And similarly for a metabolic network, in which nodes are metabolites and edges are enzyme-catalyzed metabolic reactions. These networks exist as if they are natural objects to be studied. But, does this make them free of ethical questions? Could knowing the detailed structure of a network be used to intentionally disrupt its natural function, e.g., a local food web, or the local waterways? What if the measurement of the edges requires the sacrifice of living organisms? Etc.

[1] As of September 2021, Venmo transactions are public, by default.

Discussion questions:

- Under what circumstances can it be ethical to use network data that was obtained illegally, e.g., data sets that are leaked, or shared without consent?
- Are there types of interactions that are too sensitive to even record as a network?
- What kinds of risks to individuals are created by recording a network that includes them?
- What obligations do researchers have to the individuals in these networks?
- What are the ethical tradeoffs of using digital trace information to passively observe network interactions vs. measuring interactions by obtaining informed consent from individuals?
- Under what circumstances should a researcher share vs. protect network data?

1.2 Networks leak information

Not all attributes of nodes correlate across edges in a network, but many do. And when they do, we can indirectly learn something about a particular node's attributes merely by examining the revealed attributes of its neighbors, i.e., homophily implies *guilt by association*, without needing to directly observe the individual's variable. Information about a node leaks across its edges because edges are more likely to occur if two nodes' attributes are correlated.

In most social settings, we embrace a principle of mutual autonomy across individuals—we don't get to tell our associates what information they can or cannot reveal about themselves, and they don't get to tell us the same. When this autonomy combines with the global view that a network provides of a social context, the mere presence of an edge allows our friends, family, and colleagues to probabilistically reveal information about us, and vice versa. Our association makes us a threat to our associates' private variables; in other words, privacy is a network effect. Information about a node that we gain by examining its neighbors is thus distinct from the information we might gain by directly inspecting a given node, since the node likely has more control over what it personally reveals, but not over what its associates reveal.

Examples of private information that can be "leaked" in this way include sexual orientation, political views, religious beliefs, location information, economic activity, criminal activity, lies, etc. (Can you think of more?) Of course, not all variables that exhibit homophily on a network pose specific risks if revealed; although a person may not disclose their favorite breakfast cereal, it's unlikely that inferring or revealing it would harm that individual. And, for a given variable, not all risks are the same across individuals; the risks of being outed are greater for individuals living in cultures hostile to non-heterosexual behavior. And, not all variables exhibit homophily.

The strength of homophily on any particular variable at the global level, and its covariance with other variables, sets the baseline rate at which information about it leaks across edges in a net-

work. The ubiquity of homophily implies that all information leaks on networks. In settings where networks evolve in "real time," these information leaks can enable efficient surveillance of a whole population from a relatively small number of "sentry" nodes (as in disease surveillance) or compromised nodes (as in surveillance for control).

Discussion questions:

- What distinguishes "public" vs. "private" data?
- Are some types of information okay to leak? If so, what types?
- How might we assess the degree to which some information leaks or not?
- What obligations do researchers have if they recover sensitive hidden information via network analysis? (Can you think of an example?)
- What ethical obligations do network researchers bear when developing methods that can be used to recover hidden (private) information?
- What are characteristics of network data that increase the risk of network information leaks?
- What limitations should social networking companies self-impose on using their network data to infer private information, i.e., facts about their users that their users have not disclosed?

1.3 Re-identifying networks

Like all data, network data can be persistent, transferrable, and recombinable. They can be copied and distributed widely, stored for long periods of time in multiple places, stripped of associated contextual information, lost, or combined with new information. How a network data set might be used long after it is collected is almost unforeseeable, and that makes it difficult to assess the potential harms or benefits that go along with difference choices for recording network information. Because networks are relational, every node in a network data set is potentially re-identifiable within an anonymized network, using information leaks via the edges.

In science, we often take it as a principle that data should be open and shared, so that past results can be replicated, and new results can be obtained by carrying out new analyses on old data. This idea reflects the interests of the scientific community. But if there are risks to the individuals *in the data*, this principle can (but not always) collide with the interests of individuals, to remain anonymous. Networks pose special risks for re-identification of individuals because of information leakage, because the particular set of neighbors and their attributes greatly increases the uniqueness, and thus the re-identifiability, of each node in a network.

De-identifying network data is a technical task with many solutions, not all of them sufficient, the details of which vary by the characteristics of the data (i.e., how unique is each node?) and what aspects of the data are more or less important to preserve. Too much obfuscation may alter the

results that come from running the same network analysis on the de-identified data (do you see how?), while too little may allow some or all nodes to be re-identified, even after anonymization. A persistent challenge is our natural failure to imagine risks and harms, especially from adversarial situations or unforeseen downstream uses or unanticipated "side" information.

Discussion questions:

- How does reidentification risk vary with the size of the network?
- Should de-identification aim to protect all members of the network, or just most of them?
- Which nodes are likely the most easily re-identified?
- Can an individual give informed consent for risks associated with re-identifying their neighbors?
- Under what circumstances should a researcher share vs. protect network data?
- What technical means can be used to reduce re-identification risk in networks?
- Under what conditions is simple node-level anonymity acceptable?
- What are characteristics of a network data set that increase the risk of reidentification?

1.4 Ethics and network analysis

In fact, network analysis itself poses ethical conundrums, depending on what network insights it produces and the actions or interventions those insights facilitate that would not have been possible before. For example, the large and growing literature on methods to predict missing network information, such as missing links or missing node attributes, is often motivated by addressing accuracy problems with network measurement. But, these methods are based on the tendency for information to leak across edges, and can enable the recovery of information that was intentionally hidden or omitted. Improving methods for predicting missing information can facilitate or amplify ethical problems in their use.

In fact, we might argue that *all* network analyses induce ethical questions because they provide a privileged view into the global structure of the system and enable network interventions. Here are some examples. Studies of different strategies for removing nodes or edges from a network in order to disrupt its connectivity may enable new kinds of attacks on social, biological, economic, transportation, or technological networks. Network-based vaccination strategies, which prioritize nodes with certain structural features or network positions over others, raise questions of vaccine equity and moral hazards. Methods for "aligning" two different networks in order to match nodes that exist in both could be used to create sophisticated structural re-identification attacks. And, any work on the "controllability" of a network's dynamics poses questions about how such control might be used. What other examples can you think of?

Discussion questions:

- What ethical burdens should algorithm development bear for the potential uses of those methods, e.g., to predict missing network information?
- How much burden should researchers bear to envision potential misuses of network analysis methods? Are there some areas where the burden is more or less?
- What network analyses are too risky to carry out? What analyses are inherently benign?
- How should researchers evaluate the risks and benefits associated with publishing network insights?
- How should researchers articulate the risks and benefits associated with network analyses?

2 Supplemental Readings

1. Tubaro et al., "Social network analysis: New ethical approaches through collective reflexivity. Introduction to the special issue of *Social Networks*" *Social Networks* **67**, 1–8 (2021)

2. Kosinski, Stillwell & Graepel, "Private traits and attributes are predictable from digital records of human behavior." *Proc. Natl. Acad. Sci. USA* **110**(15), 5802–5805 (2013)

3. Jernigan & Mistree, "Gaydar: Facebook Friendships Expose Sexual Orientation." *First Monday* **14**(10), (2009)

4. Radaelli et al., "Quantifying Surveillance in the Networked Age: Node-based Intrusions and Group Privacy." Preprint, arxiv:1803.09007 (2018)

5. Zheleva & Getoor, "To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles." *Proc. 18th Internat. Conf. World Wide Web* (WWW), 531–540 (2009)

6. Zimmer, "But the data is already public: On the ethics of research in Facebook." *Ethics Inf. Technol.* **12**, 313–325 (2010)

7. Backstrom et al., "Wherefore Art Thou R3579X? Anonymized Social Networks, Hidden Patterns, and Structural Steganography." *Proc. 16th Internat. Conf. World Wide Web* (WWW), 181–190 (2007).

8. Hay et al., "Resisting Structural Re-identification in Anonymized Social Networks." *Proc. VLDB Endowment* **1**(1), 102–114 (2008).