DO CIVIL SOCIETY’S DATA PRACTICES CALL FOR NEW ETHICAL GUIDELINES?

Andrew K. Woods

Prepared in advance of the “Ethics of Data in Civil Society” Conference, Stanford University, September 15-16, 2014

Introduction.........................................................................................................................................................1
1. Are Civil Society’s Data Practices Distinct Enough to Warrant Their Own Ethical Guidelines?.........................4
2. Are Civil Society’s Data Practices Uniform Enough for One Set of Ethical Guidelines?........................................6
3. Given How Quickly Today’s Data Collection, Analysis, and Norms Are Evolving, Civil Society Should Move Cautiously and Adopt Flexible Rule Design.................................7
4. Civil Society Need Not Start Anew: Civil Society Should Adapt Existing Ethical Data Principles Rather Than Create New Ones .................................................................10
Conclusion..........................................................................................................................................................11

INTRODUCTION

We live in an age of near-constant data exchange.¹ Those of us with a cell phone, an internet connection, or a credit card – those of us, that is, not fully off-the-grid – regularly volunteer digital scraps about our life, wittingly or unwittingly, to hundreds of entities that collect, store, aggregate, analyze, and monetize this data. We transmit data about ourselves over time, data about ourselves across different aspects of our life, and in aggregate data about entire populations. For nearly everyone, this data exchange has become a regular feature of life in the 21st century – a feature with significant benefits and significant costs. We have become accustomed to, if not entirely comfortable with, large and sometimes anonymous actors gathering and analyzing our data for their own purposes.

While many of these data collectors are businesses and governments, an increasing number of them – an underappreciated number of them – are members of the independent sector. In fact, data collection and analysis has become a critical component of many of the services provided by civil society groups.² Humanitarian groups now crowd-source location data to improve disaster relief;³ political campaigns use online advertising tools for more effective

¹ Data collection has become such an area of concern in the U.S., in 2014 the White House commissioned a 90-day review of so-called “big data” collection and analysis and the attendant privacy concerns. See http://www.whitehouse.gov/issues/technology/big-data-review.


fundraising, outreach, and advocacy; and gene banks collect and catalog (and even digitize) huge caches of DNA data. In some domains, such as medicine and education, aggregated data has even become a primary site of basic science and scholarly research.

These new data practices present a thicket of complex ethical questions. Consider, for example, the ethical quandaries faced by one small civil society organization, Crisis Text Line, which offers teens the chance to receive crisis counseling by text message. The service has been heralded for taking an old concept—the crisis hotline—and reconceiving it from the ground up with new technologies. Unlike crisis phone lines, the service is silent, so teens can text privately in the bathroom or in their bedroom without drawing attention to themselves. When teens contact Crisis Text Line for help, their messages are routed through the organization’s digital platform and appear on the computer screen of a trained counselor who responds as soon as possible to provide both counseling and referrals.

Because Crisis Text Line’s platform is digital, data capture is trivially easy, and this raises a set of ethical questions that an analog crisis line is unlikely to face. For instance, when teens send a text message requesting counseling, should Crisis Text Line automatically store the name and number and location of the person texting? Doing so might enable the organization to provide more personalized counseling, but it could also compromise the teen’s privacy. If that personally identifying data were to become public somehow, by accident or by theft, the damage to the teen’s privacy could be enormous. If such a breach were to occur, to whom should Crisis Text Line be accountable? What about data analysis: if the organization does decide to store data, should it aggregate and analyze that data, for example tracking different sorts of crises over time or by location? Doing so might promise to uncover patterns that would allow the organization to staff up at critical moments when crises are expected to surge. This data could also prove to be invaluable for academics and public health officials seeking to prevent teen crises. But should Crisis Text Line share its data with third parties? How do existing confidentiality regimes apply to Crisis Text Line? Are the texts that teens send to Crisis Text Line legally privileged, like some doctor-patient communications? And are Crisis Text Line’s counselors obligated, like some public agents such as teachers and 911 operators, to report suspected abuse to the police?

At the very minimum, Crisis Text Line should presumably be transparent about its plans for the data it collects. But what does that mean in practice? What kind of warning can the organization give that accurately reflects its data practices without compromising its service? If the warning is too long, or too complex, it might dissuade teens from using the service,

---


6 The Responsible Data Forum has hosted a series of timely discussions highlighting many of the ethical issues involved in civil society’s wide-ranging data practices. See https://responsibledata.io.

7 See www.crisistextline.org.

8 See Leslie Kaufman, *In Texting Era, Crisis Hotlines Put Help at Youths’ Fingertips*, N.Y.TIMES A1, Feb. 5, 2014 (noting that unlike crisis phone lines, the service is silent, so teens can text privately in the bathroom or in their bedroom without drawing attention to themselves).
precisely when they need it the most. On the other hand, if the warning is incomplete and teens later feel that they were not adequately warned, they may flee the service. This is a difficult challenge for any organization, let alone one that is communicating in short 160-character messages. Moreover, how can the organization tell teens what it plans to do with their data when it may not yet know? Data analytics change as rapidly as the technologies for data capture. Finally, if Crisis Text Line’s answers to any of the above questions are unsatisfying to a distressed teen, can that person reasonably be expected to negotiate the terms of their crisis counseling service mid-crisis?

These are striking and as-yet unresolved ethical questions faced by just one small civil society organization. But they are also familiar questions to anyone who has followed the ongoing ethical debates about data collection and analysis by corporations and governments. Every day, news headlines tell us about Facebook users upset over the latest changes to the terms of service, or American citizens seeking to learn more about the National Security Agency’s data collection and analysis. These debates feature similar questions: What data should be stored, and for how long? How should people be notified about data collection, storage, and use? How should data be kept secure? What should be done in the event of a data breach? Who should be held liable for data security? Should data be shared with third parties? Who owns the collected data? The list goes on.

As we struggle with these questions, it is worth considering whether our answers ought to vary depending on whether the data collector is a government body, a business, or a member of civil society. In other areas of life, we routinely make distinctions between government activity, private activity done for profit, and private activity done for the public benefit—distinctions, that is, between the public, private, and independent sectors. Do these distinctions make a difference for the ethics of data collection and use? To many of us, it matters whether the entity collecting data is the National Security Agency or Google. Should it also make a difference if the entity is a non-profit such as, say, Wikipedia, Khan Academy, Crisis Text Line, or the Digital Public Library of America? If it does matter, then we may need separate ethical guidelines for commercial data use, government data use, and nonprofit data use.

In many respects, the independent sector is distinctively poised to develop cutting edge, thoughtful rules for ethical data use. In stark contrast to many businesses and governments, nonprofits engender high levels of trust from the public; they are insulated from many short-term pressures; and they have generally avoided scandals of data abuse. Civil society may also have a special ethical duty regarding the data it collects—a duty that presumably warrants distinct ethical guidelines from the ones that are being developed for the other sectors. Whether such a duty exists is a debatable point, but for the purposes of this essay, let us assume that it does.

---


10 Whether such a duty exists is a debatable point, but for the purposes of this essay, let us assume that it does.
the independent sector has good reason to lead the way in developing best practices for ethical data collection, storage, and use.

But even if we accept that civil society is in a good position to develop its own ethical guidelines and that it has special ethical duties regarding the data it collects, there are practical reasons why it would be very difficult – and possibly futile – to develop new ethical guidelines for data use in the independent sector. This essay explains why. First, the essay challenges the wisdom of pursuing ethical guidelines sector by sector, suggesting that if ethical guidelines should vary at all, they should vary far more from industry to industry than across sectors. Second, the essay challenges the wisdom of pursuing new guidelines at all, arguing that civil society should move slowly, with an eye towards adopting and adapting existing ethical guidelines for data collection and use. The essay is offered as a provocation. The aim is not to offer comprehensive answers to civil society’s ethical data quandaries, but instead to identify essential questions that must be answered as part of an inquiry into sector-wide ethics.

1. Are Civil Society’s Data Practices Distinct Enough to Warrant Their Own Ethical Guidelines?

At first blush, it may seem obvious that a nonprofit’s data practices require different ethical guidelines than those that guide a for-profit organization. The nonprofit is likely to have different incentives and different aims for whatever data it collects than a for-profit organization. Crisis Text Line, for example, has very different aims for the data it collects from those of a commercial online service, like Pinterest or Facebook. In fact, Crisis Text Line would be unlikely to offer the same service on a for-profit basis, either because of insufficient revenue or low levels of trust from users, or both; the non-profit nature of the organization is essential to its service. Unlike most commercial services, Crisis Text Line almost exclusively handles extremely sensitive material. The fact that teenagers choose to use Crisis Text Line, whose very service is premised on privacy, suggests that they do not want to share this information with anyone they know. Facebook, by contrast, is designed with the opposite goal in mind – sharing information with people you know.

These two very different services, with very different institutional designs and goals, presumably ought to have different rules about how long they keep user data, whether they anonymize the data they store, whether they share user data with third parties, and more. We might expect to see different terms of service, different data policies, and different data practices. Where Facebook’s terms of service might allow it to share information with third parties – something users might even welcome as an enhancement of the online service – it seems unlikely that Crisis Text Line users would welcome the sharing of their data with third parties. This is an extreme comparison, but we can construct similar comparisons between online commerce websites, like eBay, and NGOs that collect data to assist in the delivery of

---

11 Crisis Text Line’s website boasts that text messages offer a measure of "privacy, comfort, and mobility" that phones do not. See http://www.crisistextline.org/who-we-are/our-blog/. Other text message counseling services are similarly premised on the idea that text messages offer a measure of privacy that phone calls do not. See Leslie Kaufman, supra note 8.
humanitarian assistance in the wake of a disaster. The data rules of the former are unlikely to satisfy the needs of the latter. This suggests that nonprofits’ use of data raises distinct ethical questions from those of a for-profit entity.

But in practice, can a clean line be drawn between the independent sector and the private sector? For one thing, these entities co-mingle more than ever. Nonprofit organizations routinely use commercial third party tools in their data collection, analysis, and storage. Crisis Text Line, for example, encourages teens to send very personal information by text message – data that is scooped up and recorded by private telecommunications companies. No matter how privacy-protective an NGO’s terms of service might be, and no matter how robust its security practices, if it routes data through a for-profit company, it will be subject to the legal and cyber safeguards of the host company. Not incidentally, this is something the U.S. government knows all too well. While it would be difficult for the National Security Agency to track every internet user and every single piece of internet traffic, the agency instead relies on private market tools to track this information. In the digital realm, it is increasingly difficult to go it alone, even for the NSA. Just as it is costly for the NSA to develop all of its tools in-house, it is exceedingly costly for a civil society group to collect and manage data without the use of private market tools. There may be no escape from commercial enterprises when it comes to data transmission, collection, and storage.

To make matters worse, the formal lines between different institutional forms are blurring, making it harder to separate the so-called independent sector from the rest of society. As Lucy Bernholz, Chiara Cordelli, and Rob Reich argue, for-profit and nonprofit entities can both be thought of as part of the emerging “digital civil society.” The authors write about a de jure and de facto blurring of institutional lines. As a matter of formal institutional design, for example, new corporate charters now allow B-corporations to position themselves as members of civil society. And as a matter of fact, businesses are taking on social aspirations, often referred to as social enterprises or pursuing a double bottom line, and nonprofits are taking on business strategies and outcome metrics, often seeking to generate earned revenue to wean themselves from dependence on charity. More generally, as services like Twitter and Facebook become critical tools for political mobilization, they seem less like third party partners and more like the platforms without which some civil society groups do not exist. If for profit companies are part of civil society, and those for profit companies are already engaged in a debate about data ethics guidelines, does civil society need its own data ethics guidelines?

Ultimately, data practices should vary more across different industries than across different sectors of society. Consider, for example, a nonprofit hospital and a for profit hospital: do patients at the for-profit hospital have different expectations for the collection and handling of their data than patients at the nonprofit hospital? It seems unlikely that they would. Yet patients in either hospital would surely have different privacy expectations about the data they share with their doctor as compared to the data they share with their friends via an app

---

that runs on their phone – regardless of whether the app was designed by a for-profit organization or not. In these examples, the context in which the data is collected matters more than the institutional design or tax status of the organization doing the data collecting. We have a different expectation of privacy at a hospital than we do on Facebook or when we communicate with an environmental advocacy group. Each of these very different entities raises distinct ethical questions, but it is not clear that these questions vary significantly by sector – that is, whether the group is a nonprofit, a for-profit, or a government entity. For most of us, when it comes to data ethics, a nonprofit hospital is more like other sorts of hospitals – for-profit hospitals and government-run veterans’ hospitals – than it is like a humanitarian organization, despite the fact that both are members of the independent sector.

2. Are Civil Society’s Data Practices Uniform Enough for One Set of Ethical Guidelines?

A second challenge to developing a set of ethical guidelines for data use by civil society is the enormous diversity within civil society. A humanitarian organization involved in the digital mapping of crisis zones has different ethical concerns from a food bank, a micro-loan cooperative, or a political action committee. These different entities may vary in their size, makeup, constituency, methods, goals, and much more. Each of these features may influence the data practices – and the ethical challenges – of the organization.

Consider one concrete ethical dilemma that any organization dealing with digital data must address: how long should the organization store the contact information of its clients? For an NGO engaged in community organizing and political activism, this information is its lifeblood, critical to the organization’s ongoing success. For such an organization, the answer to the foregoing question will be “as long as possible,” measured on the order of years. For a humanitarian group engaged in crisis response, this information may be risky to hold and, if lost or stolen, could compromise the integrity of the institution (not to mention violate humanitarian law). For such a group, the answer to the foregoing question will be “for as little time as possible,” measured on the order of minutes, if any personally identifying information is stored at all. Such examples multiply quickly. Given this variance, it seems quixotic to insist that all civil society groups can or should identify the same predetermined time period for storing digital data. Five days might be perilously short for some organizations, and perilously long for others.

The problem, as this example illustrates, is not a matter of rule abstraction, either. That is, one might imagine that even if the two civil society groups cannot agree to a specific rule – such as “civil society groups must destroy data after one year” – they might agree on a comparatively vaguer standard – such as “data should be kept for as little time as possible.” But in this case, the two groups are unlikely to agree even on a vaguer standard. For the organization engaged in political activism, the goal might be to store the data for as long as possible, exactly the opposite of the goal for the humanitarian group.

The length of time that personal contact data is stored is of course only a tiny piece of a much larger data ethics puzzle. Two different civil society organizations will likely have appropriately different answers to all of the following questions: How much data is
collected? For what purpose? For how long? Who owns the data? Who has access to the data? What are the barriers to others accessing the data? What is the purpose of the data? What can be done with the data? What are the appropriate anonymization measures and, relatedly, what counts as personally identifiable information? Is focused collection possible or necessary or to the contrary is bulk data collection desirable?

Moreover, different civil society organizations may come down on different sides of a debate when values clash. For example, two organizations might rightly identify different equilibrium points as they try to balance individual interests in data privacy, security, and liberty, with group or public interests in the benefits produced by the data. A medical services provider may be more protective of individual privacy, despite huge public gains from sharing individual data, where a number of other services – gene banks, political action groups, and more – may side with enhancing their service rather than protect individual privacy when faced with the choice.

3. Given How Quickly Today’s Data Collection, Analysis, and Norms Are Evolving, Civil Society Should Move Cautiously and Adopt Flexible Rule Design

There is an urgency to today’s debates about the ethics of data use and misuse. Reading accounts of these debates, one gets a sense that new rules are needed as soon as possible. Technology is changing so quickly, the argument often goes, and the stakes for privacy and security are so high, that strong guidelines must be developed immediately. The new technological and analytic tools at our disposal facilitate innovations that outstrip the old rule regime, thereby necessitating new rules.

This argument makes intuitive sense, but it is probably wrong. Given how quickly data practices are changing – and given that the stakes are so high – a strong case can be made to move cautiously and to wait before laying down firm limits on the ways data can be collected, stored, and used. There are at least two reasons to embrace this cautious approach: (1) civil society will do significant harm if it adopts the wrong rules, and (2) given the fast-changing and poorly understood nature of data analysis today, it is reasonable to assume that we may not know which rules are the right rules. The very pace of the technological change is what counsels patience rather than rapid rule change.

The wrong rules will cause harm because they will limit the significant public benefit that the new era of data collection promises. What can be done with a given data set changes every day. Strict rules for data anonymization, to give just one example, may produce enormous harm if they do not accommodate these fast-changing technologies and analytics. Imagine a gene bank that destroys personally identifying information in accordance with strict data minimization and anonymization rules. These rules may protect user privacy, but at what cost? As data analysis becomes more sophisticated, we are sure to discover connections in

---

14 See Richards & King, supra note 9 at 24 (Referring to “a sense of a crisis in personal information”).
entire populations of data and these connections could save lives. Take, for example, the healthcare nonprofit Kaiser Permanente, which used sophisticated data analysis of its electronic health records to discover that patients taking the drug Vioxx had a significantly elevated likelihood of suffering a heart attack compared to patients not taking the drug, a finding that ultimately led to the drug’s being taken off the market.\textsuperscript{16} If Kaiser had not begun storing, synthesizing, and analyzing enormous amounts of patient data across several domains – including, in this example, cardiology, orthopedics, and general medicine – this discovery may have been delayed, costing many lives. If we are overly protective of privacy, we will unnecessarily destroy data and lose the chance to make these crucial connections.

Just as the benefits of data collection are a function of what can be done with that data, so too are the possible privacy harms a function of data analytics, the capabilities of which change every day. Where hiding the names of every donor in a gene bank was once a sensible and possibly sufficient step to anonymize the database, today’s tools for analyzing metadata can render this anonymization step nearly useless. Last year, researchers demonstrated that basic online tools are enough to identify particular DNA donors in a supposedly anonymous database.\textsuperscript{17} Given that both the benefits and the costs of storing large amounts of data in centralized databases change as new technological and analytic tools are developed, it can be very hard to make a consequentialist evaluation of one policy as compared to another.

Not only is it difficult to develop sensible policies given today’s fast-changing data practices, it is difficult for an organization to be wholly transparent about its data practices. One of the challenges for any group engaged in data collection and analysis is giving people a sense of what is being done with their data. People cannot make an informed decision about their data if they do not understand what is being collected about them, by whom, and for what purpose. This is why so many efforts to devise a set of best practices for data collection emphasize notice and consent.\textsuperscript{18} This sort of transparency may be even more important for civil society, which has fewer accountability mechanisms than the corporate or public sectors. But how can a civil society group tell patrons what will happen with their data if it does not yet know what it can do with their data?

An organization’s goals might change, their data collection methods and targets might change, and they might even transfer control of the data collection to another party. Of course, the easy solution to these problems is to require that notice be given when these things change – to let people know when a new use is discovered for their data, or new data is being collected, or a new player is involved in doing the collection. This would require a second set of authorizations, and might require people to opt in if they approve of the new data practice. For some civil society groups, this may be a fine solution to the problems presented by new data capabilities. Planned Parenthood, for example, keeps track of its clients and could presumably email them or send them a letter alerting them to the fact that

\textsuperscript{17} See John Bohannon, \textit{Geneology Databases Enable Naming of Anonymous DNA Donors}, 339 \textit{SCIENCE} 262 (Jan. 2013).
\textsuperscript{18} Notice and consent are at the core of the OECD guidelines, as well as the Federal Trade Commission’s Fair Information Practice principles.
the organization is planning to do new things with the data that they collect.

But for other civil society organizations, this is either prohibitively costly or fundamentally incompatible with the goals of the organization. For organizations dealing with data from hundreds of millions of users, keeping track of up-to-date contact information could be hugely costly. It would require a system for identifying and contacting people – a system that by its very existence might threaten the organization’s efforts to keep data anonymous. Of course, data systems have been devised that aspire to keep contact information and personally identifying information separate, but efforts at anonymization have largely failed.19 An opt-out regime might be more palatable to such an organization, because huge numbers of people – those not reachable and those uninterested – will by default consent to the new use. But far from solving the problem, this scheme merely highlights the tension between what the organization wants – maximal approval of the new data practice – and the level of notice and control over their data that the individual wants.

All of this change – the evolving nature of data collection and analysis – counsels in favor of moving slowly and with flexible rule design. Moving slowly matters because the longer rule-makers take to design the right rules, and the more they know about the potential implications of their regulations, the lower the chance that the regulation will produce harmful side effects. It also counsels in favor of flexible rule design. One of the most fundamental – perhaps the fundamental – question of American constitutional law is the extent to which Constitutional values are set in stone, or whether they are meant to evolve over time.20 Designers of ethical data rules can sidestep this sort of foundational debate by clarifying from the outset that the principles are meant to evolve as the world of data collection and analytics evolves. This is true, by the way, whether the rules in question are federal laws, regulatory rules passed by an administrative agency, or voluntary principles developed by an industry group.

Rules must adapt to three sorts of changes: technological, analytical, and normative. The first sorts of changes garner the most attention. As a new technology like location-aware cellphones emerge and are adopted, they produce new data streams that can be captured, archived, and analyzed. As the technology changes, ethical data principles must adapt. Privacy standards that focus only on data and ignore metadata, like one’s location, will be inadequate to protect privacy. Second, ethical data principles must anticipate and be designed to accommodate new analytic capabilities. If a new tool allows datasets to be anonymized in a particular way – or de-anonymized in a particular way – the rules for anonymization must be written in a way to accommodate for this change. Finally, and most importantly, the rules should accommodate changing social norms. There is some early evidence – albeit anecdotal and


20 See DAVID A. STRAUSS, THE LIVING CONSTITUTION (2010). One irony of using constitutional law as an example here is that the constitution’s own privacy protections are ever-evolving, as new technologies proliferate. For a recent example, see the Supreme Court’s ruling that the 4th Amendment requires police to obtain a warrant before searching the contents of an arrestee’s cellphone. Riley v. California, 134 S. Ct. 999 (2014). See also Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477 (2006).
contested – that the use of social technologies has shifted social norms in some contexts. As one recent paper put it, “privacy… like other norms is in a state of flux.”21 Civil society can only achieve this sort of flexibility if it adopts flexible rules, rules that are designed to change as the situation changes.

4. Civil Society Need Not Start Anew: Civil Society Should Adapt Existing Ethical Data Principles Rather Than Create New Ones

It would be foolhardy to attempt to devise completely new ethical standards for civil society’s data practices, given that a number of ethical standards already exist. Instead, what is needed is a thoughtful review of how existing standards apply specially to different civil society organizations and how to make those standards enforceable. For example, there is wide agreement about the values represented in the guidelines developed in 1980 by the Organization for Economic Co-operation and Development (OECD).22 Civil society groups should determine to how to implement OECD guidelines in practice, rather than attempting to devise their own set of ethical standards from scratch.

The central values in the OECD guidelines can be summarized as follows:

1. Collection Limitation Principle (there should be limits to how much data is collected)
2. Data Quality Principle (personal data should be accurate and relevant to the purpose)
3. Purpose Specificity Principle (the purpose for data collection should be specified before or at the time of the data collection)
4. Use Limitation Principle (personal data should not be used except for the purposes specified)
5. Security Safeguards Principle (reasonable precautions should be taken to secure personal data)
6. Openness Principle (data collectors should be transparent about how, when, why, and where they collect and store personal data)
7. Individual Participation Principle (individuals should be able to inquire about and recommend changes to data stored by data collector)
8. Accountability Principle (data collectors should be accountable for complying with the above principles).

These eight principles have come to be understood as the core minimum standards for the protection of private information in the digital age.23 Of course, the OECD guidelines are not without their critics.24 Efforts to reform existing guidelines have suggested that they

21 Richards & King, supra note 9, at 21.
24 For a review of how these principles apply to big data – if not data use by civil society – see Omer Tene and Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 NW. J. TECH. & INTELL. PROP. 239 (2013).
ought to reflect, among other things, the role of encryption in security; fair treatment in public infrastructures; and the right of individuals to review and challenge the way that their data is automatically processed by algorithms. However, most of these criticisms are easily accommodated by the OECD guidelines, and a report prepared for the world’s major information commissioners concluded that debating the contents of the principles is largely an academic affair, and that efforts would be better spent at attempting to put the OECD guidelines into practice.  

The fundamental problem with these principles is that they are soft – that is, they are both vague and voluntary. They lack meaningful specificity and they lack enforcement mechanisms. Rather than carve out entirely new principles – or differently worded but largely similar principles – to the ones included in the OECD Guidelines or any of the related sets of privacy principles, civil society should direct its efforts at devising schemes to make these principles work in practice. In each industry where civil society groups participate, they might lead the way towards implementing these standards and developing mechanisms for accountability and oversight to ensure the standards are enforceable. This would be a more sensible use of civil society’s social capital than attempting to craft entirely new ethical guidelines for the entire sector.

CONCLUSION

Civil society’s collection and analysis of data is on the rise, just as it is in other sectors. Civil society’s data practices raise grave ethical concerns, to be sure, but they are largely the same concerns that arise as a result of corporate data practices and government data practices. This essay has attempted to shift the burden of proof away from a default expectation that civil society go it alone – that is, develop its own distinct ethical guidelines for data use – and towards a default expectation that civil society adopt and adapt existing data guidelines. Furthermore, the essay has provided reasons to doubt that civil society is even the right unit of analysis for data use ethics. Most of us care much more how our data is used and in what context than whether the organization using it is a member of the independent, private, or government sectors.

---

