Ethical Dilemmas in Cyberspace

Martha Finnemore

In recent years we have been busily constructing the digital world at a great pace, enjoying the many benefits it brings. Less often, however, have we stopped to think through the ethical underpinnings of these ever-expanding information and communication technologies (ICTs) or the ethics of choices embedded in the decisions we make as we build out this infrastructure and make rules about its construction and use. Questions about why we are shaping cyberspace the way that we are, as posed by Duncan Hollis and Tim Maurer in their introduction to this roundtable, often get short shrift amid our enthusiasm to embrace these technologies' latest new consumer services or military applications.

One reason for this lack of focused attention may be the fact that the governance structure for this technology is fragmented at the global level. Many of the most consequential decisions about the Internet's evolution are made in private, by (usually large) companies or national security agencies of powerful states. This limits access for most of us to engage with consequential debates about the technology's use and evolution. Figuring out how to think about the ethical issues embedded in this enterprise can be overwhelming. That is why this roundtable's strategy of focusing each essay on one strand of concern (a "prime directive" in the framing essay's terminology)—warfighting, economic gains, or freedom of expression and privacy—helps illuminate some of the ethical trade-offs and choices embedded in this build-out of ICTs. Trade-offs are ubiquitous, and it is these conflicts among values that create real ethical dilemmas for policymakers and citizens alike.

Missing from the roundtable, however, is a deep ethical examination of these "prime directives" themselves, and the largely utilitarian emphasis of the essays leaves some basic ethical questions unaddressed. In this short concluding essay,

Ethics & International Affairs, 32, no. 4 (2018), pp. 457–462.

doi:10.1017/S0892679418000576

I step back from the more detailed regulatory discussions supplied by the individual contributors to highlight three large background issues that raise fundamental ethical concerns. Some of these concerns are unique to ICTs; others have deep roots in international ethics but are only beginning to be pressed as ethical concerns about cyberspace, deserving of attention.

Are We Ends or Means?

Ronald J. Deibert's discussion of "data stewardship" raises the clearest bundle of deontological claims in the roundtable, and some of these are unique to cyberspace. As he describes, the basic business model of most big tech companies now commodifies the "data exhaust" we generate as individuals going about our daily lives online.[1] For all of the "GAFAM" companies (Google, Amazon, Facebook, Apple, Microsoft), the raw material powering their business and generating profits is the data harvested from the activities of users. *We* are the crop being harvested by these companies.

Instrumental treatment of human beings is ethically problematic in well-known ways. Ethically, people can never be means; they have ethical standing and are ends in themselves. This commodification of people—their identities, their data, their privacy—thus raises questions about the ethical basis of the business model on which all of this digitally generated wealth rests. The fact that this data collection happens without compensation, usually without the generator's knowledge, and without meaningful consent only underscores the problem, as Deibert makes clear. And businesses are not the only ones treating us and our identities in these instrumental ways. National security agencies and, of course, criminal enterprises also collect and use our data in ways we cannot control.

The data stewardship model that Deibert describes offers an ethically attractive alternative. Giving individuals control over their data, and requiring permissions for its use, could help reduce this instrumentalist and potentially exploitative power relationship. But underlying this situation is a deeper trade-off that Deibert flags: Are we willing to give up all of the "free" services generated by the current GAFAM business models that rely on free data? Indeed, much of the economic prosperity outlined in Daniel J. Weitzner's essay might be threatened by rejection of this business model. One can imagine business models in which individuals are compensated for use of their data, but the effects of such a change are hard to predict. In our complex and tightly coupled digital economy

https://doi.org/10.1017/S0892679418000576 Published online by Cambridge University Press

it is unclear what kinds of services would be economically viable, what they would cost, and who would be "priced out" of which markets. Implementing this kind of stewardship model would, itself, entail an array of ethical choices about trade-offs amid a great deal of uncertainty about outcomes.

Economic Inequality: Whose Wealth?

Founding stories about the Internet's culture in its early days emphasize Jeffersonian ideals of freedom, universal access, and participatory governance by users.[2] The Internet today, however, has evolved into something very different.

In the economic sphere, the original (relatively) egalitarian and participatory Internet structure has evolved to give us enormous, perhaps unprecedented, concentrations of wealth. Economic activity on the Internet is now dominated by some of the largest corporations in human history. Apple and Amazon have both now topped the $1 trillion mark in market valuation. Alphabet (Google's parent company) and Microsoft are within striking distance of that.[3] The inequalities of not just wealth but also power generated by ICTs in the global economy are large, and growing.[4]

Vast economic inequality is nothing new, of course, and neither are ethical concerns about it. What is surprising is how slow our ethical conversations have been to focus on the Internet as a major contributor to increasing disparities of wealth, income, and economic power. Weitzner's excellent essay is representative of the kinds of conversations we have about economic regulation of ICTs. His six foundational elements of early Internet governance all deal with *market processes* and certain types of access; they do not ponder *market outcomes*.

Ethically, outcomes should concern us. We love the goods and services free markets bring us, but markets rarely distribute benefits equally. Markets can be excellent tools for producing aggregate wealth, but they are bad at equitable distribution. We know this, yet this knowledge has not much influenced the ways we talk about Internet regulation. One could argue that this situation is simply a reflection of the current political climate. After all, enthusiasm for increasing economic equality via regulatory policy is not much evident in other spheres of the economy either at the moment, so perhaps the current situation in cyberspace is of a piece with that. But the redistribution of not just wealth but also market share and market power to a few core companies seems worth some ethical consideration.

Whose Security?

As the introduction to this roundtable explains, some of the trade-offs at stake can be drawn out by fleshing out ICT policies designed to maximize a one-dimensional goal or "good," and the place these trade-offs emerge most clearly is in the contrasting visions of the warfighting approach (offered by Hollis and Jens David Ohlin) versus the human-centric approach (offered by Deibert). These essays raise an important question: Whose security should the Internet be designed to protect—that of states or that of the people in them? Should the Internet be optimized to help states protect themselves *in extremis*, such as in times of war? Or should it be optimized to protect individual human beings, whose life and wellbeing may be threatened in a host of ways, including by their own governments?

Again, this is not a new debate in ethics. The very lively "human security" debate, on which Deibert draws, has wrestled for decades with conflicts between securing the lives and wellbeing of people, regardless of nationality, within a system of sovereign states.[5] In a human security framework, threats need not emanate from states at all. Climate change, disease, and other threats are of grave concern. But even focusing on states, as the essays here do, we can still see this ethical dilemma clearly.

The Hollis and Ohlin essay is self-avowedly statist in orientation. It embraces the statist paradigm, taking for granted that national defense and national security are unproblematic notions, ethically speaking. And, in a sovereigntist legal frame, this is loosely representative of current thinking in both law and much of security studies about states' rights and duties in conflict situations. The authors point to interesting ways in which ICTs might change states' strategic calculus, for example, around the "duty to hack" if hacking helps avert kinetic destruction, thereby protecting lives. But the more fundamental question about whether, or under what conditions, the state itself is a moral good worth protecting is not addressed.

Deibert challenges some of these notions in crucial ways. He elaborates the many ways in which governments can be threats to the security of their own citizens, and the ways in which ICTs can help governments carry out those harms. Even outside of wartime situations, states can threaten people through surveillance and other tools that make both repression of political opponents and meddling in other states' affairs easier. That said, there are also long-standing ethical arguments justifying some amount of state compromise of what would otherwise be

individual rights in the name of protecting a larger community.[6] Arbitrating this trade-off between individual and state security would seem to depend on where one comes down on larger debates about the moral standing of states and about the rights and duties of states and citizens vis-à-vis one another.

Conclusion

As the introduction to this roundtable makes clear, these essays are seminal, not definitive. Their goal is to start conversations about ethical dilemmas in cyberspace, not resolve them. ICT evangelists often present the technology sector as apolitical, advocating an ethically inert vision of technical progress. This is, of course, an illusion, and it can cause ethical concerns to be overlooked, or swept under the rug both in the construction of the architecture of these networks and in the ways we use them.[7] Ethical conversations about technology thus are often slow to catch up with engineering and have trouble driving or controlling changes in ways we might like. But the ubiquity of these technologies makes catching up imperative. We do not talk about ethics in cyberspace enough, and these essays are a helpful prompt to change that.

NOTES

[1] "The World's Most Valuable Resource Is No Longer Oil, but Data," *Economist*, May 6, 2017, www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. But see Bernard Marr, "Here's Why Data Is Not the New Oil," *Forbes*, March 5, 2018, which emphasizes the variety and "renewable" nature of data, both of which add to its power, www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#5215a1a73aa9.

[2] David G. Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (New York: Oxford University Press, 2009).

[3] Laura Stevens and Amrith Ramkumar, "Amazon Hits $1 Trillion Valuation," *Wall Street Journal*, September 4, 2018, www.wsj.com/articles/amazon-hits-1-trillion-valuation-1536075734; and Michael Sheetz, "These Are the Next Companies Poised to Hit $1 Trillion," *CNBC Markets*, August 3, 2018, www.cnbc.com/2018/08/03/these-are-the-next-companies-poised-to-hit-1-trillion.html.

[4] Drew DeSilver, "U.S. Income Inequality, on Rise for Decades, Is Now Highest Since 1928," *Fact Tank*, Pew Research Center, December 5, 2013, www.pewresearch.org/fact-tank/2013/12/05/u-s-income-inequality-on-rise-for-decades-is-now-highest-since-1928/.

[5] Roland Paris, "Human Security: Paradigm Shift or Hot Air?" *International Security* 26, no. 2 (2001), pp. 87–102; and Amitav Acharya, "Human Security: East versus West," *International Journal* 56, no. 3 (2001), pp. 442–60.

[6] Richard A. Falk, *Human Rights and State Sovereignty* (New York: Holmes & Meier, 1981); Louis Henkin, "Human Rights and State 'Sovereignty,'" *Georgia Journal of International and Comparative Law* 25, no. 1 (1996), p. 31; and Astri Suhrke, "Human Security and the Interests of States," *Security Dialogue* 30, no. 3 (1999), pp. 265–76.

[7] Cees J. Hamelink, *The Ethics of Cyberspace* (London: Sage, 2000), pp. 6–8.

Abstract: This essay steps back from the more detailed regulatory discussions in other contributions to this roundtable on "Competing Visions for Cyberspace" and highlights three broad issues that raise ethical concerns about our activity online. First, the commodification of people—their

https://doi.org/10.1017/S0892679418000576 Published online by Cambridge University Press

identities, their data, their privacy—that lies at the heart of business models of many of the largest information and communication technologies companies risks instrumentalizing human beings. Second, concentrations of wealth and market power online may be contributing to economic inequalities and other forms of domination. Third, long-standing tensions between the security of states and the human security of people in those states have not been at all resolved online and deserve attention.

Keywords: cyberspace, ethics, data stewardship, economic inequality, human security, national security, sovereignty

https://doi.org/10.1017/S0892679418000576 Published online by Cambridge University Press