Social and Ethical Behavior in the Internet of Things

By Francine Berman, Vinton G. Cerf
Communications of the ACM, Vol. 60 No. 2, Pages 6-7
10.1145/3036698
Comments

Last October, millions of interconnected devices infected with malware mounted a "denial-of-service" cyberattack on Dyn, a company that operates part of the Internet's directory service. Such attacks require us to up our technical game in Internet security and safety. They also expose the need to frame and enforce social and ethical behavior, privacy, and appropriate use in Internet environments.

Social behavior and appropriate use become even more crucial as we build out the "Internet of Things" (IoT)—an increasingly interconnected cyber-physical-biological environment that links devices, systems, data, and people. At its best, the IoT has the potential to create an integrated ecosystem that can respond to a spectrum of needs, increasing efficiency and opportunity, and empowering people through technology, and technology through intelligence. At its worst, the IoT can open a Pandora's Box of inappropriate and unsafe behavior, unintended consequences, and intrusiveness.

The difference between an IoT that enhances society and one that diminishes it will be determined by our ability to create an effective model for IoT governance. This model must guide social behavior and ethical use of IoT technologies while promoting effective security and safety. While we should not limit technology innovation too early with overly restrictive policy, neither should we leave the policy and governance discussion until the IoT is so mature that it cannot easily incorporate protections.

What Policy Will Be Needed for the IoT?

Although much of the policy needed for the IoT may evolve from Internet governance, the scale, heterogeneity, complexity, and degree of technological autonomy within the IoT will require new thinking about regulation and policy and force new interpretations of current law. As an example of the complexity of the governance challenge, consider three key areas critical to ensure the positive potential of the IoT:

1. What are your rights to privacy in the IoT? The IoT will sharpen the tension between individual privacy and the use of personal information to promote effectiveness, safety, and security. Who should control information about you? Who should access it? Who can use it? The answer is not always clear-cut. Consider medical monitoring devices and the information they accumulate. Should your personal health information be shared when the Centers for Disease Control want to track a potential epidemic? When bio-medical researchers want to model potential treatment strategies on a richer dataset? When an employer is considering you for a job?

At present, policy and laws about online privacy and rights to information are challenging to interpret and difficult to enforce. As IoT technologies become more pervasive, personal information will become more valuable to a diverse set of actors that include organizations, individuals, and autonomous systems with the capacity to make decisions about you.

Some have suggested that individuals should have a basic right to opt out, delete, or mask their information from systems in the IoT, providing one tenet of a potential IoT "Bill of Rights." However, it may be infeasible or impossible for an individual to control all the data generated about them by IoT systems.

Interestingly, strong individual privacy rights may also mean less social benefit. Too many "opt-outs" may erode the public and private value of IoT datasets,[3] negatively impacting their social benefit—imagine a Google map where locations come and go. The complexity of providing useful services subject to dynamic participation and evolving individual preferences may be extraordinarily complex to develop and administer.

2. Who is accountable for decisions made by autonomous systems?As autonomous systems replace some human activities, we face the challenge of when and how these systems should be deployed, and who is responsible and accountable for their behavior. When your "smart" system fails, is hacked, or acts with negative or unintended consequences, who is accountable, how, and to whom?

A high-profile example of this is autonomous vehicles, which make many decisions without "a human in the loop." We currently expect automobile companies to be accountable if automotive systems, such as anti-lock brakes, fail. As cars begin to drive themselves, who should be responsible for accidents? As systems take on more decisions previously made by humans, it will be increasingly challenging to create a framework for responsibility and accountability.

3. How do we promote the ethical use of IoT technologies? Technologies have no ethics. Many systems can be used for both good and ill: Video surveillance may be tremendously helpful in allowing senior citizens stay in their homes longer and parents to monitor their newborns; they can also expose private behavior to unscrupulous viewers and unwanted intrusion.

In his highly popular and visionary books, Isaac Asimov posited four laws of robotics[1,2] on the basic theme that robots may not harm humans (or humanity), or, by inaction, allow humans (humanity) to come to harm. Asimov's Laws provide a glimpse into the social and ethical challenges that will need to be addressed in the IoT. How do we promote and enforce ethical behavior by both humans and intelligent systems? Will we need to develop and incorporate "artificial ethics" into automated systems to help them respond in environments when there are good and bad choices? If so, whose ethics should be applied?

Toward a Framework for Thinking About Principles and Policy for the IoT

What might a general IoT governance model look like? In 2008, the Forum for a New World Governance developed the "World Governance Index" (WGI) focusing on peace and security, democracy and the rule of law, human rights, development and participation, and

sustainability. These areas provide a roadmap for considering IoT governance. Mapping the WGI areas to the IoT indicates that we will need:

- *Policy for IoT safety, security and privacy*, requiring the development of viable approaches promoting individual rights, data security, and trust, as well as disincentives and penalties for inappropriate behavior, corruption, and crime.
- *A legal framework for determining appropriate behavior* of autonomous IoT entities, responsible and accountable parties for that behavior, and determination of who can enforce compliance, how, and on what grounds.
- *Focus on human rights and ethical behavior* in the IoT, including a sense of how these would be enforced. This gets to the heart of the need for the IoT to promote human well-being and contribute to the advancement of society.
- *Sustainable development of the IoT* as part of a larger societal and technological ecosystem, including its impact on biological systems (for example, 3D-printed organs, implants), environmental systems, and natural resources).

We need to lay the groundwork now. The IoT should advance society and not just technology. The first step is to pursue the discussions, studies, task forces, commissions, and pilots that will help develop governance for an empowering and enabling IoT. Developing policy and legislation in newsworthy and opportunistic areas (for example, transportation) is essential, but not enough. We need to be thinking deeply *now* about broad IoT use and deployment, and how it can help create a more enlightened and civilized society. If we wait too long, we do so at our own risk.

Authors

Francine Berman is the Edward P. Hamilton Distinguished Professor in Computer Science at Rensselaer Polytechnic Institute, Troy, NY. She is an ACM Fellow.

Vinton G. Cerf is vice president and Chief Internet Evangelist at Google. He served as ACM president from 2012–2014.