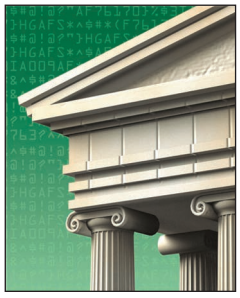
Editor: Virgilio A.F. Almeida • *virgilio@dcc.ufmg.br*



A Principles-Based Approach to Govern the IoT Ecosystem

Virgilio A.F. Almeida and Benjamin Goh • *Harvard University*

Danilo Doneda • *Rio de Janeiro State University*

The difference between a good and bad Internet of Things depends on society's ability to construct effective IoT governance models. This article proposes the formulation of principles as a means to unify the multiple bodies and organizations involved in the IoT governance ecosystem.

With the attack on Dyn in 2016, the Internet of Things' security and its potential impact on the Internet are once again in the spotlight.[1] The Dyn attack, aimed at the Internet's domain name server (DNS) infrastructure, disrupted multiple major service providers, including Twitter, Netflix, Spotify, Airbnb, Reddit, and *The New York Times*.[2] In a public announcement in September 2015, the FBI warned about the use of IoT devices and the potential virtual and physical threats they might pose.[3] As Vint Cerf emphasized,[4] the difference between good and bad IoT depends on society's ability to construct effective IoT governance models. In this article, we discuss ideas for the development of the IoT governance ecosystem.

IoT's logic arises primarily from tech companies, who wish to use increased connectivity to market products that provide greater convenience and more personalized services. Amazon's Alexa, Google's driverless car, and the Fitbit Flex are all products that ride this new wave of digital convenience. However, beyond the consumer level, IoT applications are increasingly used in industries, such as energy management systems, industrial automation, and in management of urban facilities, such as smart grids and smart traffic lights. Used in this way, IoT poses serious cybersecurity issues, creating "new risks in complex ecosystems."[5] Such IoT systems create new risks around privacy and security protections, especially when they're used in mission-critical systems. In essence, IoT applications amplify vulnerabilities in existing software and hardware.

To ensure safety, security, and privacy in the IoT ecosystem, governments, civil society, the private sector, and academia must be at the table to discuss new governance mechanisms that minimize the risks introduced by IoT. The consequences of delaying the construction of rules, norms, and regulations for IoT are potentially catastrophic.

Minimizing or Mitigating IoT Security Threats

There's no doubt that IoT services provide services and efficiency that can improve welfare. However, it opens up new levels of vulnerabilities that raises further governance questions: for example, while ISPs used to be the only one able to retrieve web browsing history from someone's personal WiFi, the explosion of devices connected through the home can now reasonably predict a person's activities at home, raising new privacy and security concerns. Security researchers at Princeton University found that "the contents, patterns, and metadata of network traffic can all reveal sensitive information about a user's online activity."[6] In particular, they found that even with encrypted traffic, a network observer can use network send/receive rates to tell if a user is sleeping, or if there's a change in frequency of motion to determine if the house is occupied or if guests are coming.[6]

Published by the IEEE Computer Society 1089-7801/17/$33.00 © 2017 IEEE

The US Federal Trade Commission's (FTC's) 2015 staff report on IoT classifies security threats in the following three ways:

- enabling unauthorized access and misuse of personal information;
- facilitating attacks on other systems; and
- creating safety risks.[7]

First, the risk to unauthorized access and misuse of personal information isn't new, especially if you consider the vulnerability of social media accounts from being compromised, or that a USB inherently has insecure design flaws.[8] However, IoT creates a new urgency to the problem, because an individual's security is only as strong as the weakest link, and an IoT system might create more opportunities for "lateral movement" to compromise someone's security. Whereas it might be convenient for us to rely on our phones for all IoT services (such as thermostats), malware that infects smartphones might compromise our safety at a scale larger than before.[9]

Second, IoT devices are, by definition, devices that have the ability to connect to the Internet. Thus, vulnerabilities in any IoT device have the potential to become an attack vector through which a malicious actor causes harm to others. The most popular form of such vulnerabilities come in the form of the Mirai botnet, which takes advantage of industry negligence toward IoT devices to compromise devices for nefarious use.[1]

Third, new dependencies are created by IoT services, which can create new sources of risk to human safety. The US Food and Drug Administration (FDA) found that pacemakers and defibrillators by St. Jude Medical contain cybersecurity risks that make them highly vulnerable to attack, potentially affecting the lives of tens of thousands of patients with cardiac devices.[10] Security researchers have also famously shown how they could remotely compromise the Chrysler Jeep Cherokee's entertainment system, rewrite its firmware, and control the car by sending commands to critical systems (such as the brakes).[11]

Security and privacy protection are key for a "good" IoT. However, IoT applications create different types of privacy risks. Smart TVs, for example, through beaconing technology and cross-device tracking, allow all home devices to share information without our knowledge. Along these lines, Amazon recently agreed to hand federal courts data gathered from an Echo speaker to assist in investigations in a murder case.[12] It isn't clear how much information the Amazon Echo collects, but it also raises important questions about privacy — is the home still "private," or does one forgo privacy protections by purchasing an Echo? Finally, distinct from privacy risk is the IoT's potential in creating surveillance risks. Whereas privacy is most famously defined by Louis Brandeis to be the "right to be left alone," surveillance risks occur when the government has an abundance of tools to monitor individual behavior. In the Berkman Klein Center's *Don't Panic* report, for example, the authors found that metadata is unlikely to become encrypted, which provides government officials a wealth of data such as "location data from cell phones and other devices, telephone calling records, and header information in e-mail" that can fuel surveillance.[13]

The IoT Governance Ecosystem

The IoT governance ecosystem has many players with very different legal statuses. They operate on many different layers on municipal, national, and international levels, driven by technical innovation, user needs, market opportunities, and political interests. The specific form of each component of the ecosystem must be designed according to the very specific needs and nature of the individual issue. There's no "one size fits all" solution for IoT governance.

Many agencies and organizations deal with guidelines and regulation of IoT devices. On the municipal level, the City of New York[14] has proposed a common framework to help agencies develop policies for IoT with the following goals:

- provide a common framework to help governments develop and expand policies and procedures related to the IoT;
- ensure openness and transparency regarding the use of public space or assets for smart city technologies; and
- advance the public dialogue about how government, the private sector, and academia can collaborate to ensure these technologies are used in a way that maximizes public benefit.[15]

An example of a municipal rule for IoT is "All IoT devices and network equipment installed on city property should have clear site license agreements and established terms of service governing who is responsible for ongoing operations, maintenance, and the secure disposal of equipment."

On the national level, many countries have initiatives to create regulations and standards for IoT applications. In the US, several agencies — including the Food and Drug Administration, the Federal Communications Commission, the FTC, and the National Highway Traffic Security Administration — are reviewing some aspects of IoT.[16] As the technology moves into healthcare, and data from wearable health devices flows more from consumers' wrists to companies, the Food and Drug Administration (FDA) is keeping interest in the evolution

of IoT applications. The US Department of Energy (DOE) established the Federal Smart Grid Task Force, with experts from 11 different federal agencies to coordinate strategies to promote integration of smart-grid technologies and practices. At the international level, different organizations have proposed guidelines and standards for the IoT. The Internet Society (ISOC),[17] the IETF,[18] and the International Telecommunication Union (ITU)[19] have published reports and recommendations of technical standards to enable IoT on a global scale.

IoT Governance Principles

So, out of this a natural question arises: What could be used to "glue" different groups and interests together in a global IoT governance ecosystem? Even considering the importance of IoT governance, the way it can be structured is absolutely open for debate. Nonetheless, the vectors this structure shall follow can be drawn from the reflection utterly made in the face of the development of governance tools to act on the Internet environment. Common principles could be the element that will put together different interests in an environment in an inclusive, effective, and legitimate governance framework. They could contribute to contextualizing the IoT as part of global resources that should be managed in the public interest. In this sense, we chose a set of applicable principles developed in the NETmundial Multistakeholder Conference.[20]

Governments and several stakeholder groups, including civil society, private sector, and academia, gathered to discuss issues and principles for Internet governance and roadmap actions for the Internet's future evolution. Among the issues discussed, the scope of Internet governance was preeminent, in the sense of the tension between those who see Internet governance as a mostly technical matter (with, for example, IP numbers, routing and specifications, DNS, and critical resources) and others who approach Internet governance as something that must comprehend and factor important social and political issues, such as privacy, freedom of expression, and human rights in a general sense.

The final result, the NETmundial Declaration, encompassed principles both of a technical nature as well as non-technical ones. Some of these principles can be deemed as guidance to IoT governance, as a relevant part of IoT's impact can be related to them. For example, one principle refers to the structure of the Internet governance ecosystem, which should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community, and users. This principle reiterates the importance of having civil society representatives in governance bodies. In the case of IoT, this should be a key principle, in particular because of the massive presence of IoT devices on the consumer side. Two other principles could be used in the construction of the global IoT governance ecosystem: first, governance models should be open, participative, transparent, and consensus-driven; and second, Internet governance should be carried out through a distributed, decentralized, and multistakeholder ecosystem.

Issues related to security and privacy rise to the fore as IoT's influence permeates our daily lives. Such issues then reflect onto the NETmundial principle about privacy that states, "The right to privacy must be protected. This includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data" (www.netmundial.org/principles). This principle encompasses data protection as well. In fact, to the extent that IoT provides for a vast number of devices to be connected to the Internet, it happens that several of them gather personal data. Many of them are strictly sensors that are responsive to personal activities. This makes for a concrete increase in the volume of personal data gathered. It also makes the case regarding what these devices can do: they collect far more personal data than is reasonably expected, deemed fair, or authorized, and they proceed to the treatment of the personal data they collect with low security. These two points are linked to another characteristic tendency of IoT, which is the proliferation of small and simple devices, in general too simple and cheap to include safeguards about excessive and unfair collection of personal data or to implement data security at a reasonable level.

Eventually, these IoT weaknesses can be addressed through a conjunction of other principles present in the NETmundial declaration, particularly the principles of accountability and transparency. And, moreover, there's the fact that the IoT per se exponentially expands the number of devices attached to the Internet (often small and cheap ones) and these devices, if expected to comply with privacy and security rules, shall be submitted to technical standards that emphasize this compliance. In this sense, some of the Internet governance principles of the NETmundial Declaration can be used as a basis to assemble interested stakeholders in an open and participative dialogue for constructing the IoT governance ecosystem.

References

1. N. Woolf, "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say," *The Guardian*, 26 Oct. 2016; www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

2. N. Perlroth, "Hackers Used New Weapons to Disrupt Major Websites Across U.S.," *The New York Times*, 21 Oct. 2016; www.nytimes.com/2016/10/22/business/internet-problems-attack.html
3. US Federal Bureau of Investigation, *Internet of Things Poses Opportunities for CyberCrime*, Alert Number I-091015-PSA, 10 Sept. 2015; www.ic3.gov/media/2015/150910.aspx.
4. F. Berman and V.G. Cerf, "Social and Ethical Behavior in the Internet of Things," *Comm. ACM*, vol. 60, no. 2, 2017, pp. 6–7.
5. European Commission's High Level Group of Scientific Advisors, *Cybersecurity in the European Digital Single Market*, scientific opinion no. 02, Scientific Advice Mechanism, European Union, 24 Mar. 2017; https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf.
6. N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home Is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," US Federal Trade Commission (FTC), 2016; www.ftc.gov/system/files/documents/public_comments/2016/10/00022-131586.pdf.
7. FTC, *Internet of Things: Privacy & Security in a Connected World*, FTC staff report, 2015; www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
8. J. Condliffe, Jamie. "USB Has a Fundamental Security Flaw That You Can't Detect." *Gizmodo*, 31 July 2014; http://gizmodo.com/usb-has-a-fundamental-security-flaw-that-you-cant-detec-1613833339.
9. R. Brandon, "App-Installing Malware Found in over 1 Million Android Phones," *The Verge*, 30 Nov. 2016; www.theverge.com/2016/11/30/13792846/googlian-android-malware-install-app-security.
10. US Food and Drug Administration, "Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin FDA Safety Comm.," FDA safety comm., 9 Jan. 2017; www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.
11. A.C. Estes, "Hackers Have the Power to Remotely Hijack Half a Million Chrysler Cars," *Gizmodo*, 21 July 2015; http://gizmodo.com/hackers-have-the-power-to-remotely-hijack-half-a-millio-1719233440.
12. I. Smith, "Amazon Releases Echo Data in Murder Case, Dropping First Amendment Argument," *PBS News Hour*, 8 Mar. 2017; www.pbs.org/newshour/rundown/amazon-releases-echo-data-murder-case-dropping-first-amendment-argument/.
13. U. Gasser et al., *Don't Panic: Making Progress on the "Going Dark" Debate*, tech. report, Berkman Center for Internet & Soc., Harvard Univ., 2016; https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
14. The New York City Mayor's Office of Technology and Innovation, *NYC Guidelines for the Internet of Things*, Sept. 2016; www.nyc.gov/iot.
15. D. Castro and J. New, *Everything the U.S. Government Is Doing to Help the Private Sector Build the Internet of Things*, tech. report, Center for Data Innovation, Information Technology & Innovation Foundation, 12 Dec. 2016.
16. M. Ravindranath, "Who's in Charge of Regulating the Internet of Things?" *NextGov*, 1 Sept. 2016; www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/.
17. *The Internet of Things (IoT): An Overview - Understanding the Issues and Challenges of a More Connected World*, white paper, The Internet Society, 2015; www.internetsociety.org/doc/iot-overview.
18. A. Keränen and C. Bormann, "Internet of Things: Standards and Guidance from the IETF," *IETF J.*, Apr. 2016; www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf.
19. V. Almeida, "The Evolution of Internet Governance: Lessons Learned from NETmundial," *IEEE Internet Computing*, vol. 18, no. 5, 2014, pp. 65–69.
20. W. Kleinwächter and V. Almeida, "The Internet Governance Ecosystem and the Rainforest," *IEEE Internet Computing*, vol. 19, no. 2, 2015, pp. 64–67.

Virgilio A.F. Almeida is a faculty associate at the Berkman Klein Center for Internet and Society at Harvard University, and a professor in the Computer Science Department at the Federal University of Minas Gerais (UFMG), Brazil. His research interests include cyber policies, large-scale distributed systems, the Internet, and social computing. Almeida has a PhD in computer science from Vanderbilt University. Contact him at virgilio@dcc.ufmg.br or valmeida@cyber.law.harvard.edu.

Benjamin Goh is a master's in public policy candidate at the John F. Kennedy School of Government, Harvard University. His research interests surround cybersecurity strategy, and the appropriate role of government in the digital world. Goh graduated with BS degrees, summa cum laude, with double honors in economics and international relations from New York University. He was named the Ellie and David Werber Research Scholar in Social Sciences at NYU, and received the Fiona McGillivray Prize for his thesis on the political economy of Internet surveillance. Contact him at Benjamin_Goh@hks17.harvard.edu.

Danilo Doneda is a professor of civil law at the Law School of the Rio de Janeiro State University (UERJ). His research interests include private law and regulation, privacy, and data protection. Doneda has a PhD in civil law from UERJ. Contact him at danilo@doneda.net.