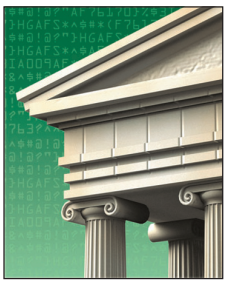
Editor: Virgilio A.F. Almeida • virgilio@dcc.ufmg.br



Governance Challenges for the Internet of Things

Virgilio A.F. Almeida • *Federal University of Minas Gerais, Brazil*

Danilo Doneda • *Rio de Janeiro State University*

Marília Monteiro • *Public Law Institute of Brasília*

Before citizens and consumers can trust the infrastructure of the Internet of Things (IoT), they must feel that their personal data are protected. Thus, legal frameworks regarding data protection will need to be adjusted.

The future will be rich with sensors capable of collecting vast amounts of information. The Internet will be almost fused with the physical world as the Internet of Things (IoT) becomes a reality. Although it's just beginning, experts estimate that by the end of 2015 there will be around 25 billion "things" connected to the global Internet. By 2025, the estimated number of connected devices should reach 100 billion. These estimates include smartphones, vehicles, appliances, and industrial equipment. Privacy, security, and safety fears grow as the IoT creates conditions for increasing surveillance by governments and corporations. So the question is: Will the IoT be good for the many, or the mighty few?

While technological aspects of the IoT have been extensively published in the technical literature, few studies have addressed the IoT's social and political impacts.[1,2] Two studies have shed light on challenges for the future with the IoT. In 2013, the European Commission (EC) published a study[2] focusing on relevant aspects for possible IoT governance regimes. The EC report identified many challenges for IoT governance – namely privacy, security, ethics, and competition. In 2015, the US Federal Trade Commission (FTC) published the FTC Staff Report[3] *The Internet of Things: Privacy and Security in a Connected World*. Although the report emphasizes the various benefits that the IoT will bring to consumers and citizens, it acknowledges that there are many risks associated with deploying IoT-based applications, especially in the realm of privacy and security.

One way of addressing these concerns is to think of IoT governance mechanisms. Thus, here we discuss some issues associated with governance of the IoT.

Risks for Citizens and Consumers

The recent development of privacy and data protection legislation can be seen as a function of scale. As the amount of personal data that's gathered and processed increases, new services and possibilities for their use are brought to life. Meanwhile, the way we think and feel about privacy isn't static. Historically, this movement caused the privacy and data protection regulatory framework to reinvent itself each time there was a major change in the quantity of personal data possible to be processed. Automated data processing caused classical privacy legislation to develop into the data protection legal frameworks now present in several countries.[4]

In the IoT, where objects interact between themselves without requiring human commands, people are also affected. Even in the case of applications that don't directly target human beings, such as an industrial process in a factory, indirect information about humans can be collected and inferred. For a vast number of cases, the availability of devices and sensors in an environment can drastically increase the amount of personal data being gathered. That contributes to blurring the boundaries between a "physical world" and cyberspace, in the sense that many actions we perform will be monitored, recorded, and used.

 Published by the IEEE Computer Society 1089-7801/15/$31.00 © 2015 IEEE

In fact (and more specifically), the boundaries between IoT and surveillance may also blur and, ultimately, vanish if initiatives to protect privacy aren't in place. The negative impact of IoT on society may be aggravated as data from sensors are used together with personal data already available, and foster a number of correlations and data crossings that can performed without any kind of control. This will also be facilitated by the increasing efficiency of techniques of re-identification of anonymized data.

Increasingly we see that IoT is, in fact, directly related and intertwined with human beings.[5] In its opinion on IoT, the Article 29 Working Party — a group of European data protection authorities — has focused on three developments of IoT that relate directly with the rights of individuals: wearable devices, quantified self (devices that track and record aspects of someone's life), and dobotics (devices with sensors used in home automation).

Some emerging privacy issues are related to the spread of sensors, particularly because their use will result not only in more data being collected but also in the increasing accuracy of the collected data. In this sense, for example, a movement sensor present in a smartphone is often precise enough to capture delicate patterns of its user's movement, producing data that can be used to evaluate his health, habits, and so on, with an unprecedented degree of precision. Another example is in the automobile industry, with the increased computing in cars[6] that makes it possible to register driver's every moves. While such data could make driving safer and more efficient, it also can become a source of sensitive information about the driver, her habits, her physical condition, and so on. There are similar dilemmas in several other examples, such as with smart meters in smart-grid applications, and in projects of so-called smart cities. In short, IoT allows for deeper scrutiny of individuals than ever before.

The plethora of potential risks posed by IoT isn't restricted at all to privacy ones, as strict security risks can be identified as well. For instance, in the case of smart cities, where sensors can control almost everything, from water management to power networks, hackers and attackers may find vulnerabilities to harm large parts of cities. Other risks could be directly related to individuals[4] — such as risks from misusing and manipulating IoT objects. Examples include manipulating the critical driving elements of a smart car or medical connected devices that provide a patient with precise doses of medicine.

Principles to Protect Citizens and Consumers

To protect citizen's personal data and to build people's trust in the IoT infrastructure, legal frameworks regarding data protection must be adjusted according to the nature of these new technologies. Let's focus on four principles that we can use to construct rules and norms for deploying IoT applications:

- notice and choice;
- data minimization;
- access to personal data; and
- accountability.

The notion of notice and consent is one of the most intricate to work with. Its general formulation refers to a statement and a menu of choices presented to the citizen to decide how she would like her data handled. In IoT, though, there's hardly any formal interface between sensors and citizens. In addition, attempts to build a traditional notice and choice environment could lead to failures, due to the scale and capillarity of the IoT sensors and devices.

The lack of user interface and the sheer number of sensors makes traditional notice and choice systems difficult to implement in IoT, and the fact that there's an increasing number of actors in the IoT ecosystem who might be able to access sensor data (for instance, on several occasions, its manufacturers) shall compel IoT applications to explore various possibilities to provide citizens with meaningful information about the data being gathered, who is responsible for it, and how citizens can easily demand their rights about these data.

The principle of data minimization — collecting as little personal data as possible — is usually regarded as paradoxical with IoT, where sensors generally monitor as much data as possible. A standard sensor generally aims for simplicity and energy efficiency, focusing on gathering data in an efficient way. This leads to the question of whether data that can be collected must be collected. Given the difficulty to regulate the gathering of data by sensors with little capacity to limit themselves, attempts to exercise this kind of control will be directed to other elements of the IoT ecosystem. This also raises questions about liability for designing and controlling data collections systems. Those involved should be accountable for data misuse.

Going a bit further, other elements and actors in IoT governance can be called to their duties. As stated in the EC report,[2] there's widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices. Also, rigorous security validity checks, authentication procedures, and data verification will be part of the foundation of IoT applications. The inclusion of the manufacturers in the IoT regulation process depends on a global view that includes not only IoT norms and rules but also the privacy governance process in cyberspace.

As with any other personal data collected by third parties, personal data monitored by IoT devices must

Organization Names and Acronyms

The following are a list of names and acronyms for some of the organizations mentioned in this article.

ICANN	Internet Assigned Numbers Authority
IETF	Internet Engineering Task
IGF	Internet Governance Forum
ISOC	Internet Society
RIR	Regional Internet Registries
W3C	World Wide Web Consortium

be available to the data owner in order for him to exercise his right of access. This is only possible when there's transparency in the data collection process, along with clear indications of who is responsible for data treatment in the IoT ecosystem.

In this sense — in recognizing the need to provide accountability for the several actors present in the IoT ecosystem — some options are being considered, such as the introduction of trusted third parties (eventually located outside IoT ecosystems) that can provide for information and also gather the options and consent of citizens whose personal data might be collected and used.

Role of Governance in IoT

A classical definition for Internet governance[7] is the development and application by governments, the private sector, and civil society (in their respective roles) of shared principles, norms, rules, decision-making procedures, and programs that shape the Internet's evolution and use. The question that naturally arises is: Does the IoT need new mechanisms for its governance, or are the existing Internet governance bodies[8] and rules sufficient? It seems evident that IoT governance shouldn't be discussed in a separate or isolated way from the general Internet. Several IoT problems (such as security, interoperability standards, and protocols) might have solutions through the implementation of governance mechanisms, as occurs with the general Internet. One possible path to the future is to broaden the discussion around IOT governance, involving multistakeholder groups, in order to represent multiple views on IoT problems and issues. The existing Internet governance ecosystem (IETF, ICANN, RIRs, ISOC, IEEE, IGF, and W3C) is an adequate space to discuss IOT-related governance issues.

The nature of privacy and security problems[4,9] frequently associated with the IoT indicates that further research, analysis, and discussion are needed to identify possible solutions. First, the introduction of security and privacy elements in the very design of sensors, implementing Privacy by Design, must be taken into account for outcomes such as the homologation process of sensors by competent authorities. Even if the privacy governance of IoT can oversee the control centers for collected data, we must develop concrete means to set limits on the amount or nature of the personal data collected.

Other critical issues regard notification and consent. If, from one side, it's true that several sensors are already collecting as much personal data as possible, something must be done to increase citizens' awareness of these data collection processes. Citizens must have means to take measures to protect their rights whenever necessary. If future scenarios indicate the inadequacy of a mere notice-and-consent approach, alternatives must be presented so that the individual's autonomy isn't eroded.

As with other technologies that aim to change human life, the IoT must be in all respects designed with people as its central focus. Privacy and ethics aren't natural aspects to be considered in technology's agenda. However, these features are essential to build the necessary trust in an IoT ecosystem, making it compatible with human rights and ensuring that it's drafted at the measure, and not at the expense, of people.

References

1. R.H. Weber, "Internet of Things – Governance Quo Vadis?" *Computer Law & Security Rev.*, vol. 29, 2013, pp. 341–347.
2. European Commission, *Report on the Consultation on IoT Governance*, tech. report, 16 Jan. 2013; https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.
3. Federal Trade Commission, *Internet of Things, Privacy & Security in a Connected World*, FTC Staff Report, Jan. 2015; www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
4. V. Mayer-Scönberger, "Generational Development of Data Protection in Europe," *Technology and Privacy: The New Landscape*, MIT Press, 1997.
5. Article 29 Data Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, tech. report, 16 Sept. 2014; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
6. Telefonica, *Connected Car Industry Report 2013*, Telefonica, 2013, p. 9; http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.
7. Working Group on Internet Governance, *Report of the Working Group on Internet Governance*, tech. report, WGIG, June 2005, p. 4; www.wgig.org/docs/WGIGREPORT.pdf.
8. V. Almeida, D. Getschko, and C. Afonso "The Origin and Evolution of Multistakeholder

Models," *IEEE Internet Computing*, vol. 19, no. 1, 2015, pp. 65–69.
9. M. Enserink and G. Chin, "The End of Privacy," *Science*, 30 Jan. 2015, pp. 490–491.

Virgilio A.F. Almeida is a professor in the Computer Science Department at the Federal University of Minas Gerais (UFMG), Brazil. His research interests include large-scale distributed systems, the Internet, social computing, and cyber policies. Almeida has a PhD in computer science from Vanderbilt University. He's the chairman of the Brazilian Internet Steering Committee (CGI.br). Contact him at virgilio@dcc.ufmg.br.

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.

Marília Monteiro is a researcher from the Center of Law, Internet, and Society at the Public Law Institute of Brasília (CEDIS/IDP). Monteiro is an MPP candidate at the Hertie School of Governance (Germany), and she holds an LLB from the Getulio Vargas Foundation School of Law. Contact her at m.monteiro@gmx.com.