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

Privacy Governance in Cyberspace

Danilo Doneda • *Rio de Janeiro State University*

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

Cyberspace is the processing, manipulation, and exploitation of information; the facilitation and augmentation of communication among people; and the interaction of people, information, and devices.[1] The main characteristic of cyberspace is the interconnection of computers, information, devices, and people. Many actors are involved in cyberspace's construction and operation – namely, telcos; application, service, and content providers; users; and governments. The issue of privacy protection is a global challenge that requires a global response. The regulation of privacy in cyberspace depends on regulatory, technical, and social factors. Multistakeholder mechanisms can be a promising way to deal with privacy policies in global cyberspace.

Cyberspace plays a vital role in integrating the economic, political, social, and cultural fabric of society, and is strategically important for most nations. However, individual nations govern the central part of global cyberspace, using deeply varied strategies within local Internet ecosystems. Generally, governance of cyberspace involves a large number of actors and organizations that exceeds by far the number of usual players involved in Internet governance, such as ICANN, ISOC, RIR, IETF, W3C and IAB (we define these and other organizational names and acronyms in the related sidebar).[2] Joseph Nye[3] provides a partial map of governance activities in cyberspace, which includes international law conventions (for example, the UN Charter and UNGA), government groups (G20 and OECD), telecom regimes (ITU), human rights organizations (Human Rights Watch), law enforcement cooperation (Interpol), intellectual property regimes (WIPO), civil rights organizations (EFF), trade regimes (WTO), and intelligence community alliances, such as the *Five Eyes*.

Almost every aspect of modern life is being rapidly transformed by the innovative ways cyberspace is collecting, organizing, analyzing, using, and disseminating information. National ID numbers, social security numbers, bank accounts, credit cards, and smartphones provide identification and tracking of the places where a person has been or is. Furthermore, Facebook posts, Instagram pictures, tweets, Google searches, and surveillance cameras are able to reveal your behavior, thoughts, interests, and worries. The combination of powerful computational techniques (for example, machine learning algorithms) and vast amounts of personal data can lead to instances of privacy invasion. In summary, the technological evolution of cyberspace has drastically changed the notion of individual control over the disclosure and use of personal information. As a consequence, privacy is always a topic of interest in Internet and cyberspace governance discussions and concerns. Here, we analyze various aspects of privacy governance in cyberspace and point out the importance of personal data protection as a concrete means for implementing effective privacy protection frameworks around the world.

Privacy in Cyberspace

Developing privacy safeguards has never been the subject of a real global coordination initia-

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

tive and this can be for a number of reasons. Indeed, privacy is hardly a homogeneous concept. Its subjective character makes it rather difficult to establish a concept of privacy that's both broad enough to encompass its several manifestations and specific enough to be really useful – which is, in fact, the only reason to bring a concept into life. Even some of the most widespread concepts of privacy – for instance, that of the "right to be let alone," although being a milestone, only catches part of its actual significance. Thus, privacy ended up being conceived and enforced by Law in a variety of ways, relying on legal frameworks and tools that are particular to each country's legal system and with no real urge for global coordination.[4]

Things changed as digital technology turned out to be the real driving force behind the evolution of the concept of privacy. Adding computer power to the processing of personal data was crucial to shift the notion of privacy to a kind of "new dimension" that includes the control of the data people produce and, thus, the very notion of data protection. By protecting privacy through personal data control it became possible not only to build more concrete and effective enforcement tools, but also to work on a clear set of rules regarding data collection and processing. After all, it's not merely an open concept that should be enforced. It's a concrete movement that opens a new perspective on the international arena regarding privacy protection and governance.

By and large, the concept of privacy is specific to a country, to a culture, and to an historical period, and privacy rights generally encompass the set of these cultural and historic aspects tied to this concept. For instance, the development of the right to abortion in United States is related to privacy rights, while in continental Europe that has never been the case. As for data protection, it's a more pragmatic approach, under the rationale that it aims to safeguard individuals by protecting something that's exterior to them – their personal data. Furthermore, rules to govern data can be much more concrete and bound for global harmonization than privacy rights.

In fact, the very formulation of early data protection statutes reveal an unprecedented dialogue between international sources in an array of informal and, probably, spontaneous cross-references. The interesting phenomenon of convergence among data protection legislations is, to a certain extent, independent of any central coordination. Colin Bennett[5] observed that with factors such as technological determinism (in the sense that technical standards adopted in many countries tend to be similar), the need to emulate standards and interoperability for cross-border data flows created a demand for laws that share a common core, principles, and enforcement tools.

Even in data protection laws, we see the interesting event of convergence among different national laws that's true in some general aspects, such as the data protection principles or the establishment of data owners' rights. If we add to legislation the set of other elements to be taken into account, such as the implementation of technologies, industry's best practices, and even the different degrees of enforcement of data protection laws provided by Data Protection Authorities (DPAs), we can conclude that it is, indeed, possible to have completely different outcomes in enforcement even with similar legislation in place.[6]

Privacy Isn't Dead

The move from privacy in the cyberspace to data protection as the dominant legal framework has much to do with an emphasis on informational control and auto-determination. Thus, some notions traditionally linked to privacy, such as solitude, reclusion, and secrecy – the very "right to be let alone" – gave room to new systems where personal data can be gathered and used, as long as it follows its owner's will and expectations. So, decisions regarding sharing and disclosure of personal data can be seen not as an antithesis to privacy but

Organization Names and Acronyms

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

EFF	Electronic Frontier Foundation
Five Eyes	Alliance of Australia, Canada, New Zealand, the United Kingdom, and the United States
G20	Group of Twenty, a forum representing the 20 major economies
IAB	Internet Architecture Board
ICANN	Internet Assigned Numbers Authority
IETF	Internet Engineering Task
IGF	Internet Governance Forum
ISOC	Internet Society
OECD	Organization for Economic Co-operation and Development
RIR	Regional Internet Registries
UNGA	United Nations General Assembly
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society
WTO	World Trade Organization
W3C	World Wide Web Consortium

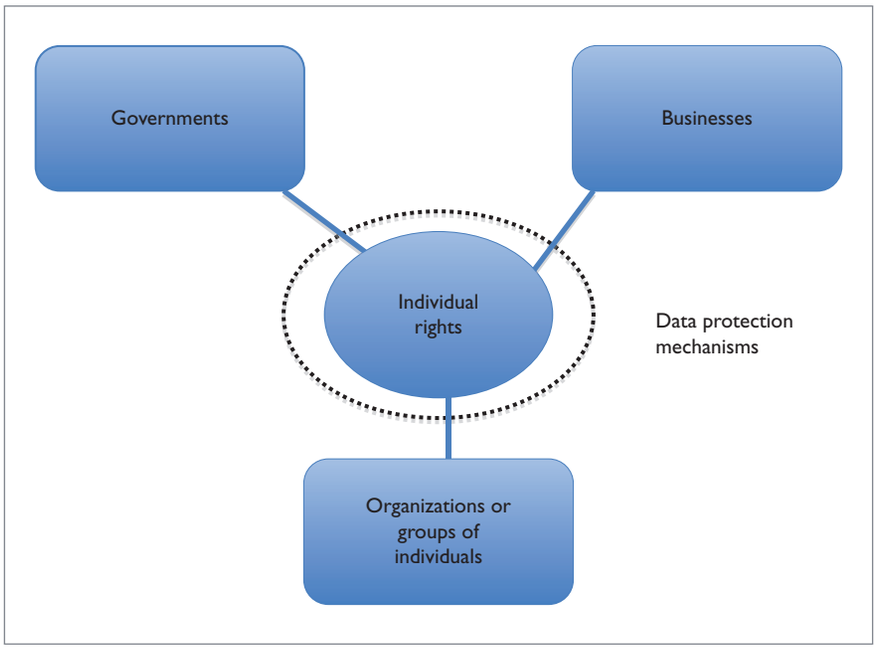

Figure 1. Privacy governance in cyberspace. Data protection should be achieved through laws and practices that encompass the information collection activities of these three main actors.

rather as legitimate decisions about the flow of someone's personal data, encompassed in a data protection framework, based on individual autodetermination and revealing one of privacy's main goals: to help preserve the individual's personality.

The emphasis on control is much more than a theoretical move. Today, the gathering of personal data seems to be, in an ever-growing set of situations, inevitable. Technologies such as sensors in smart environments, Big Data, Internet Protocol version 6 (IPV6), Internet of Things, and healthcare applications ensure that personal data gathering is ever increasing, and that regulation must include innovative tools to manage use of personal data to provide citizens effective control over their information.[7]

News regarding privacy's death, which has been repeated for decades, seems to be greatly exaggerated. Data protection's experience shows that privacy isn't merely about excluding or banning some person or information from all public contact or disclosure, but rather the management and fine-tuning of an individual's exposition to the world. In this context, a new approach to privacy governance can be conceived by linking not only the regulation concerning privacy and data protection, but the whole set of factors that helps provide interaction between the individual and the world. So, adding to regulation, factors such as technology (for example, Privacy by Design and Privacy-Enhancing Technologies) and business's best practices are the elements that will ultimately define citizens' perception of privacy.

Data Protection Implementation

Figure 1 depicts the structure of the main actors involved in privacy governance in cyberspace. For several purposes, governments collect massive amounts of personal data from their nationals and also from foreigners. In the Internet economy, businesses keep collecting data about customers, such as preferences, profiles, and navigation behavior. Groups of individuals (for example, political or religious groups) also collect information from their constituents. Data protection should be achieved through laws and practices that encompass the data collection activities of the three main actors of cyberspace: governments, businesses, and civil society. Regulators are facing a hard time in trying to encompass a set of different demands for data protection, like topics that are basically related to the nature of cyberspace, such as jurisdiction or the issue of the right to be forgotten (R2BF) and its implementation. These difficulties point to the need of alternative types of agreement, such as the formation of multistakeholder bodies to help privacy governance in cyberspace.

When data protection rules began to be put in place, it became feasible to create clear rules for handling personal data — rules that are easier for businesses to understand and comply, rules that could, with some effort, be built into products and services conceived with privacy safeguards planted deep into their code, and finally, rules that could facilitate interoperability and international standardization. This gives room to an ecosystem with characteristics that are indeed familiar when dealing with cyberspace issues. For instance, we can see the regulatory and enforcement system, the technological aspects, and the autoregulation mechanisms as parts of a structure of privacy governance in cyberspace that we can approach in a variety of ways.

Currently, we can't identify any global actor that actually enforces data protection in global cyberspace. Several important efforts are merely regional and act mostly through a regulatory approach (for example, the Article 29 Working Group and the European Data Protection Supervisor in the European Union), and some tend to be at the global level but usually lack means for actual enforcement, such as the OECD Guidelines or

the Convention 108 of the Council of Europe. Some interesting documents on harmonization have been issued, such as the Declaration of Madrid, issued in 2010 in the International Conference of Privacy and Data Protection Commissioners. Both create conditions for stronger international cooperation between DPAs. Several provocative issues are now pointing to the need of privacy and data protection mechanisms to be discussed at the cyberspace governance level. In fact, on one side, experience shows the ineffectiveness of approaching privacy issues from the viewpoint of Internet governance (which considers basically only technological issues related to privacy) — and on the other side, it shows the limitations of a purely regulatory approach. Purely regulatory approaches can lead to situations such as the recent trial by the European Court of Justice about the R2BF, whose outcome might not be as broad as its plaintiffs' desire.

The opportunity to build multistakeholder mechanisms that deal with data protection and privacy policies in the global cyberspace should be explored in light of alternative ways that put the different actors and interests together on the negotiation table. Multistakeholder approaches could be a promising alternative to privacy governance, for they have worked well for several other issues related to the evolution of Internet and cyberspace governance.[2]

Acknowledgments

We would like to thank Marília de Aguiar Monteiro for the valuable insights and suggestions.

References

1. D. Clark, "Characterizing Cyberspace: Past, Present, and Future," working paper, MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), version 1.2, 12 Mar. 2010; http://ecir.mit.edu/index.php/research/working-papers/112-characterizing-cyberspace-past-present-and-future.
2. 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.
3. J.S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities*, paper series no. 1, The Global Commission on Internet Governance, May 2014; www.cigionline.org/publications/regime-complex-managing-global-cyber-activities.
4. J.Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *Yale Law J.*, vol. 113, no. 6, 2004, pp. 1151–1221.
5. C. Bennett, *Regulating Privacy, Data Protection and Public Policy in Europe and the United States*, Cornell Univ. Press, 1992.
6. K.A. Bamberger and D.K. Mulligan, "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices," *The George Washington Law Rev.*, vol. 81, no. 5, 2013, pp. 1529–1664.
7. M. Enserink and G. Chin, "The End of Privacy," *Science*, 30 Jan. 2015, pp. 490–491.

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

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.