: Global Governance Spotlight
6 | 2014

sef:

Internet Governance and the Protection of Privacy.
Which way forward?

Rolf H. Weber

Herbert Marcuse (One-Dimensional Man) posed the question a good 50 years ago: "Can a society which is incapable of protecting individual privacy even within one's four walls rightfully claim that it respects the individual and that it is a free society?" Protection of privacy, then, has not become an issue only with the advent of electronic communications. On the contrary, non-disclosure, as demanded (in vain) by Lohengrin from Elsa, has been vulnerable to traitors and hackers since time immemorial – a fact to which other folk tales bear eloquent witness. Did Ali Baba come by the password "Open Sesame" legally, or was he the first hacker in history? In Grimm's fairy tale, did the miller's daughter, who later became queen, find out Rumpelstiltskin's name through the proper channels? A fact which cannot be ignored, however, is that in today's digital world, the risks to data privacy are very much greater, at least in a quantitative sense.

Internet governance: a new field of regulation

In view of the tension which exists between information-sharing and the protection of privacy, there is a need for the legislator to intervene by setting rules and addressing potential conflicts of interest. Due to the free movement of information, these legal interventions must focus on protecting the persons affected. The key principle in this context is "to protect people not places" (US Supreme Court in its judgment in Katz v. United States, 1967), which has led to what Martin Walser has described as "a new love of silence".

Informational self-determination

The concept of "informational self-determination" – as the practical manifestation of data protection rights at the personal level – is about the individual's right of disposition over information pertaining to them. It means that the individual should be able to decide for themselves whether and how personal details are publicly disclosed and the parameters in which this occurs. The right of data privacy is thus concerned with the classification of information as private property if, and to the extent that, it is of a personal nature.

The Internet has resulted in a greater need – primarily in a quantitative, rather than a qualitative sense – for guarantees of privacy. Companies' and citizens' growing demand for information and the broader scope for governments to make use of information, sometimes coupled with a somewhat careless approach by individuals towards the disclosure of personal data, make it difficult to protect privacy in the information age. The degree of complexity is further increased because information is often available globally, in contrast to the relevant regulatory regimes, which – in accordance with the principle of sovereignty – are generally established at the national or, at best, regional level (e.g. the European Union).

Norm-setting for the protection of privacy

The protection of privacy is addressed in various multilateral conventions (e.g. the Universal Declaration of Human Rights), but the relevant provisions are general and non-binding. Given that reaching agreement on global rules – notwithstanding the limitless opportunities for information-sharing – seems unrealistic in many areas, new forms of norm-setting must be considered.

The most important regulatory approach for the information society is based on the concept of broad-based Internet governance. At the second World Summit on the Information Society (WSIS) in Tunis in 2005, the international community agreed on the following working definition of Internet governance: the development and application by governments, the private sector, the academic and technical communities and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. The concept can also be defined as an ongoing process of discourse and consultation on how the Internet should be coordinated, managed and developed. Taking it a step further, Internet governance can be said to comprise all mechanisms, institutions and processes that organise and regulate Web-based activity.

In the last 20 years – in other words, not only since Snowden's disclosures – the protection of privacy has regularly featured on the agenda of international conferences, especially within the Internet Governance Forum (IGF) framework. It has become apparent, in this context, that topics such as protection of privacy cannot be governed solely on the basis of multilateral agreements ("hard law"). Although soft law lacks binding legal status, and universally applicable procedural principles have yet to be developed, the complexities of cyberspace require new legislative approaches and new forms of law. "Informal" law-making via a multi-stakeholder system that includes all interested Internet users offers better prospects of long-term success.

A multi-stakeholder concept as part of "Internet-ional law"

Given the significance of global information-sharing, the participation of Internet users in decision-making processes aimed at establishing the requisite legal frameworks is key. Civil society's participation in (informal) rule-setting is essential in safeguarding transparency in decision-making and guaranteeing public confidence in the outcomes.

In recent years, the "multi-stakeholder" concept has come to the fore. In essence, it conforms to the description of Internet governance given above, and involves, albeit not definitively, various "groups" of information society stakeholders. However, there are two problematical areas which cannot be ignored:

(1) It is essential to clarify the term "in their respective roles". This issue merits discussion because the current regulatory regime for the Internet is based on a confusing mass of transnational, national, association-based and private provisions. Clearly, different forms of participation are required depending on the issue to be addressed; more participation by civil society is needed, for example, in addressing the issue of personal profiles than in developing security systems to guard against cybercrime.

(2) Defining the relevant stakeholders from national governments, international organisations and the business community is a fairly straightforward process. It is much more difficult to define the representatives of civil society, which comprises an almost impossibly large number of individuals, often with highly diverse or conflicting interests. New forms of cooperation are needed for this area.

International treaties and transparency

International treaties should not be negotiated behind closed doors: that was the lesson learned from the failure of the Anti-Counterfeiting Trade Agreement (ACTA), which was abandoned by governments after widespread public protests. A more promising approach is to allow civil society representatives to have a say and to involve all interested Internet users.

Implementing a multi-stakeholder concept is therefore a learning process and is likely to take time. Nonetheless, experience with the Netmundial conference in São Paulo in late April 2014 shows that establishing appropriate structures is by no means impossible. For many stakeholders, the processes are unaccustomed; the fact that government representatives are expected to wait in line, just as civil society representatives do, for a chance to use the microphone and are given the same amount of speaking time is certainly not the traditional way of conducting negotiations. Nonetheless, the discussions at Netmundial proved more fruitful than the international negotiations at the World Conference on International Telecommunications (WCIT) in Dubai in 2012, for example.

Interoperability of regulatory regimes

The global information society would face fewer legal obstacles if regulations were harmonised on a transnational basis. However, experience shows that in relation to the protection of privacy, this is an unrealistic goal. Differences of opinion stemming from social and cultural factors make it impossible to conclude relevant multilateral treaties. Although this is a sobering assessment, it does not mean that abandoning all attempts to improve the level of protection would be the right approach.

In its Digital Agenda 2014-2017 (Chapter VI. 2), the German Government therefore rightly voices its commitment to a "high level of modern data protection" in order to guarantee the freedom and right to privacy of citizens in the digital environment. In pursuit of this approach, Germany, together with the Government of Brazil, submitted a draft resolution to the United Nations in late 2013 calling for the right to privacy in the digital age to be recognised and upheld under international law. Furthermore, in Resolution 68/167, the UN General Assembly requested the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications. The report, which has been available since 30 June 2014, focuses especially on the right to protection of privacy against arbitrary or unlawful interference by States. It also deals with the issue of procedural safeguards and possibilities of judicial remedy in response to such interference by States.

Geographical vs. organisational approach to regulation

Instead of the geographical approach to regulation (as envisaged in the EU's Data Protection Directive), which is currently widespread and aims to ensure a comparable standard of protection of personal data when transferred to third countries, more consideration should be given to an organisational approach. This would oblige the data holder to ensure, prior to any processing and transmission of information, that comparable standards are upheld in any third country where the data are accessed. This approach marks a shift away from an abstract "country comparison" towards a transfer of responsibility to the data holder and, therefore, towards the principle of accountability.

The protection of privacy is affected not only by State interference but also by private data collection. New forms of data processing, such as cloud computing, create new risks, without adequate measures currently being in place to mitigate them. Big data analytics opens up another minefield in both qualitative and quantitative terms; the vast amount of information could potentially allow the re-anonymisation of personal data. Given the diversity of data protection standards existing in various countries and the affordability of transnational data transmission, it is essential to ensure that "regulatory competition" does not result in a (further) decline in data protection standards.

The way forward: challenging but viable pathways

Although harmonised global regulations pertaining to the protection of privacy are unlikely to be within reach in the short to medium term, efforts currently under way in international organisations to improve data protection regimes must be intensified. In the absence of agreed and binding principles, the establishment of a minimum level of protection in the form of soft law may have at least a certain moral and ethical effect. Furthermore, heightened public sensitivity means that governments cannot simply ignore the issue of data protection.

In additional to regulatory regimes, there must be a greater focus on technical security solutions. Technology to guard against the misuse of data exists and is viable, although there are still some issues with its design, often making it complex to manage. In order to safeguard privacy on the Internet, greater use must be made of encryption technology; independent auditing of development-capable protection mechanisms is another important step. Restoring individuals' technological sovereignty is essential and may

The interoperability of regulations

The interoperability of regulations, discussed above, has the potential to facilitate communication, innovation and business processes, and should be pursued via various challenging but viable pathways. Firstly, more intensive efforts should be made, both within the framework of existing organisations such as the United Nations and through declarations by ad hoc organisations (e.g. Internet Governance Forum, Netmundial), to strengthen basic rights such as the protection of privacy. Secondly, self-regulation, especially by stakeholder companies, is essential. Even if soft law is non-binding, at least initially, this form of rule-making can have positive resonance and provide a starting point for the subsequent development of universal standards.

well set limits not only to the collection of content and metadata by service providers but also to data analysis by intelligence agencies, which is becoming ever more prevalent.

In recent years, many companies have realised that compliance with minimum data protection rules is a matter of concern to many market players. Confidentiality in information-sharing and data processing is thus becoming a quality indicator for product and service companies, and may even give rise to some form of quid pro quo. Companies are therefore likely to have an ever-increasing interest in contributing to data privacy by establishing their own internal data protection standards.

Individuals themselves must also take greater care of their own data. Often, personal data are disclosed with very little thought for the consequences. The heightened sensitivity to these issues, now apparent in the public debate, is therefore a step in the right direction. However, more education and training on how to interact with the digital world appear to be essential in moving towards technological sovereignty.

Author

Professor Rolf H. Weber | Chair in Civil, Commercial and European Law at the University of Zurich.

His fields of research are Internet governance and information technology law, international commercial law, telecommunications, media and competition law, and international finance regulation.

Further information

Bygrave, Lee A.: Data Privacy Law. An International Perspective, Oxford, 2014.

Kulesza, Joanna: International Internet Law, London/New York, 2012.

Weber, Rolf H.: Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles, Zurich, 2014.

Imprint

The Development and Peace Foundation was founded in 1986 on the initiative of Willy Brandt. As a cross-party and non-profit-making organisation, the SEF provides an international high-level forum for shared thinking on urgent peace and development issues.

Global Governance Spotlight is a policy-oriented series whose purpose is to critique international negotiation processes from a global governance perspective.

Published by
Development and Peace Foundation/
Stiftung Entwicklung und Frieden (SEF)
Dechenstr. 2 : 53115 Bonn : Germany
Phone +49 (0)228 959 25-0 : Fax -99
sef@sef-bonn.org : www.sef-bonn.org

Editor
Sabine Gerhardt
Dr Michèle Roth

Translation
Hillary Crowe

Design Basic Concept
Pitch Black Graphic Design
Berlin/Rotterdam

Layout
Gerhard Süß-Jung

Contents do not necessarily reflect the views of the publisher.