Privacy and International Compliance: When Differences Become an Issue

Dennys Antonialli

University of Sao Paulo Law School, Brazil (LLB)
Bucerius Law School/WHU Otto Beisheim School of Management, Germany (Master of Law and Business)
Berliner Tor 3 – Zm. 1203D
20099 Hamburg, Germany
dennys.antonialli@law-school.de

Abstract

This paper introduces key issues to the balance between data collection policies and privacy protection initiatives in an internationally unstructured legal framework. The right to privacy has been addressed and construed differently among jurisdictions, which leads to uncertainties regarding the cross-boarding data collection operations that often occur in the cyberspace. This paper focuses on the jurisprudence of the Brazilian Supreme Court, demonstrating (i) that the traditional approach given to privacy in Brazil is not accurate enough to deal with the new threats which arise in the cyberspace; (ii) that the concept of privacy should be redefined when applied to the cyberspace and; (iii) that differences among national privacy legislations challenge international compliance with regard to the right to privacy.

The traditional concept of privacy of the Brazilian Supreme Court[1]

In the last ten years, the Brazilian Supreme Court has been mostly confronted with the right to privacy in cases related to bank secrecy and wiretapping. These are cases that require the Brazilian Chief Justices to define under which circumstances privacy violations can be considered lawful. As every other fundamental right, privacy cannot be construed in an absolute way and violations might be accepted when safeguarding the public interest or the public order. Criminal persecution is a great example of this since privacy cannot exclude the conduction of investigation proceedings. If privacy did not have any limitations, one could never be searched.

Having faced the right to privacy in such cases, the Brazilian Supreme Court has formulated an interpretation which is mainly based on the approach of a *negative liberty*. In this sense, the right to privacy only entitles individuals to prevent others from interfering in their *private sphere* of life. According to this interpretation, privacy violations occur whenever facts or elements which belong to one's private sphere of life are arbitrarily accessed or disclosed. Although useful in some cases, this concept does not define what is within the boundaries of the so called *private sphere of life*, making it difficult to draw the line between what is protected and what is not. Thus, each violation is considered separately and the focus is on the level of intimacy present in the collected information.

The increasing number of activities that take place on the internet brings to the cyberspace a considerably high amount of information about its users. Being difficult to define which data are public and which data are private, the applicability of the Brazilian Supreme Court's concept of privacy becomes problematic in the cyberspace for the following reasons:

a-) "Violation-oriented" approach: this interpretation privileges a right to *resist* or to *avoid* arbitrary interferences in an individual's life. Hence, the right to privacy only serves the purpose of protecting people against possible violations. This approach is not sufficiently accurate to protect internet users from data collection since their data are often collected clandestinely, making it hard for the users to exercise their right of protection. If privacy is a right to *resist* and not a right to *control*, how can a user *resist* something that he/she is unaware of? Violations can be fought only when they are known. Taken as a mere right to *resist*, privacy does not fulfill the needs of internet users, whose data are mostly silently collected (spywares, cookies, web bugs, phishing, etc.). If the notion of *control* over personal information is not incorporated into the concept of privacy, violations will keep occurring without being fought.

[1] In order to define the traditional concept of privacy applied by the Brazilian Supreme Court, a research has been made regarding the decisions which contained the keywords "privacy", "intimacy" and "private life" in the last ten years (from 1998 until 2008).

b-) Violations are determined by an isolated analysis: in order to determine whether or not a privacy violation has occurred, the Brazilian Supreme Court analyzes if elements of an individual's private sphere of life have been unlawfully disclosed or accessed. Some pieces of data that are separately collected in the cyberspace might not represent a violation by themselves. Isolated, a piece of information might not reveal any private element of one's life. However, once the data is collected, it can be easily crossed or gathered, which substantially increases the likelihood of violation. By analyzing each and every violation separately, the negative liberty approach is unable to detect and prevent future threats.

Take the example of data concerning online shopping habits in different websites. Knowing that person X usually purchases books related to criminal law might not represent a privacy violation (the attendant of the bookshop could also observe that). Knowing that person X usually purchases medicines against asthma might not represent a privacy violation either (the drugstore attendant could also notice that). Finally, knowing that person X usually purchases bottles of shampoo against hair loss might not represent a privacy violation either (a hairdresser might also have this information). Applying the concept of privacy offered by the Brazilian Supreme Court, the conclusion is that none of these cases represent a privacy violation since these *isolated* pieces of data do not disclosure any information that belongs to the private sphere of life. Nevertheless, once these pieces of information are gathered (and in the internet they can easily be), one could know that the same person X is probably a criminal lawyer who suffers from asthma and is trying to fight hair loss. The violation becomes much more noticeable.

This power of crossing and gathering information is one of the factors that make privacy protection in the cyberspace so complex. Moreover, data collection operations in the internet happen on a rolling basis and in a very fragmented way. Building complete customers' profiles, for instance, has been a market for many companies and this practice is excluded from the scope of protection of privacy in the negative liberty approach.

The necessity of redefinition of the concept of privacy

The aforementioned issues demonstrate that privacy in the cyberspace cannot be taken as a negative liberty. The mere right of *resisting* violations (freedom from unreasonable search) does not protect the users against isolated data collections.

Therefore, privacy should be conceived as a sort of *positive liberty,* in the sense that users should be entitled to an actual *power of control* over their data. This concept is much more useful since it allows users to control the collection of any piece of their personal data, regardless of its private or public character. It does not matter whether or not a violation has occurred: if a piece of data is collected, notification and authorization of the user are required due to an actual *power of control* rather than the mere *power to resist*.

Although this notion of *information control* has proved to be more accurate to protect privacy in the cyberspace, there are still two main relevant issues that jeopardize its application:

a-) No power of negotiation: it is not difficult to realize that internet users do not have a power to negotiate their privacy preferences in the cyberspace. It is common that websites are not displayed properly if cookies are blocked or that purchases cannot be concluded if the user disagrees with the website privacy policy. In this sense, it is fair to say that users cannot truly exercise a control over their data as their disagreement or their refusal to accept privacy policies often derail further steps or activities. The architecture of the cyberspace represents an obstacle to achieving a real power of control.

b-) No control over collected data: collected data can be easily crossed over, passed on or even sold in the internet. This means that the user's control over them is equally easy to be lost. This is especially true with privacy policy clauses which state that changes might happen at any time, allowing the company to stop complying with the agreed policy at its own convenience. Even if a company states that the collected data will not be passed on to other companies, there is still no guarantee for the user that this policy will not change over time or that a different treatment will not be given to his/her data in the future. "Facebook" has recently implemented major changes in its privacy policy, obliging users to review their personal privacy settings, clearly illustrating the uncertainty in the field.

Due to these challenges in the application of the concept of information control, there have been some attempts to give privacy a new interpretation, according to which it should be elevated to the condition of a *property right*. Under this approach, a user would not only be entitled to control his/her data but would be considered as the *owner* of his/her personal data. This concept becomes particularly useful – and challenging – when it comes to sales of collected data. As it is widely known, only the *proprietor* of a good is entitled to sell it. In this sense, if pieces of data are considered goods and users are their owners, they would be the only ones who are legally entitled to trade data. Yet innovative, the concept faces serious problems of implementation since data are transferred and collected all the time in the cyberspace. It would be inefficient and overly bureaucratic to apply the rules of international sale of goods to online transfers of personal data.

Both approaches make it crystal clear that the main issue that must be solved is not *whether* internet users should be able to control the flow of their own data, but *how* this control can be exercised. Certainly, huge problems of

implementation arise with the use of existing legal frameworks, such as the transfer of property rights.

Cross-boarding uncertainties

The aforementioned concepts of privacy demonstrate that different jurisdictions might approach this right under different perspectives. The lack of harmonization regarding privacy was not very problematic before the internet. However, cyberspace is a cross-boarding reality and, since there is no standardized treatment which shall be given to privacy matters, it is very hard for online businesses and internet service providers to comply with all these conflicting approaches at the same time.

The argument can be easily illustrated by the use of the so-called "worms", small files that can dig into the hard disk of the computer seeking for specific information. When – and if – the "worm" finds the information it is looking for, it reports it back to its sender, otherwise, it self-destructs.

As a strategy for fighting counterfeiting, a company could take advantage of these files and send them through the internet, searching for illegal copies of certain software, for instance. If an illegal copy is found, this information is reported back to the company, identifying the machine on which the software is installed. If not, the worm simply destructs itself without representing any noticeable inconvenience to the operations of the investigated computer.

It has to be stated that the "inspection activity" of the "worms" is not based on any probable cause or evidence of the commitment of a crime. It is similar to the case of sniffer dogs at airports: travelers do not need to open their suitcases and reveal what they are carrying unless the dogs sniff something suspicious. However, everyone must submit their luggage to the examination of the dogs. The same happens with the "worms". Everyone has its computer searched, but a report is only sent if an illegal copy is found.

This possibility of general search, including non-suspects, is a question that often divides scholars as it affects the privacy of all citizens. But the issue that must be addressed here is that even though national legislations diverge on the topic, worms can be sent unrestrictedly through the web. This means that even if general search is forbidden according to one national law, national users might receive worms in their computers seeking for all sorts of information. Therefore, there is a challenge of international compliance when it comes to privacy.

Recently, many Brazilian users were surprised with a small star on the desktop of their computers. The star warned that an illegal copy of an operating system had been found and that the computer had been identified. In this sense, one could ask: if the Brazilian Supreme Court has not reached a consensus regarding the possibility of investigating someone without a probable cause, was it lawful to send "worms" to Brazilians?

How could businesses comply with all the national legislations in regard to general search and privacy if they wanted to adopt a single international anti-piracy strategy? How can online businesses comply with all the different approaches given to privacy in different jurisdictions when designing their privacy policies which are going to be enforced throughout the world?

Cloud computing is another great example of privacy compliance uncertainty. When users decide to store their information in servers accessible worldwide, they are giving away their data to a company which is usually not located in their home country. If their data is stored abroad, which national law should govern privacy matters: the one of the place where the server is hosted or the one of the country the user lives in?

These are examples which demonstrate that this is a deadlocked debate. There is not only a tension between privacy and control but also a tension between the different national legal concepts of privacy and the necessity to comply with all of them at the same time. Neither businesses can be sure that they are in compliance with the privacy concepts adopted by the courts all over the world, nor can the users be sure that their own national legislation is being complied with by internet service providers and online companies. The solution companies found was to set their own privacy policies to avoid these asymmetries. Yes, companies comply with what *they* came up with.

Conclusion

The limitations of national concepts of privacy such as the Brazilian one and the uncertainties that arise when different approaches to privacy are given in a cross-boarding reality suggest that an internationally more structured legal framework in regard to privacy is required in order to ease and guarantee worldwide compliance.

It is clear that the internet poses new and important challenges to the study of the right to privacy, which can be roughly summarized as:

(i) the creation of a cross-boarding cyberspace, which puts the territorial application of law into question, making it impossible to comply at the same time with different legal treatments given to the right of privacy;

(ii) the increasing number of activities that take place on the internet has turned cyberspace into an arena where more and more private information is shared by its users;

(iii) the possibility of silent and illegal collection of personal data, without the consent or even without the awareness of the users, who have their personal information captured and clandestinely transmitted online;

(iv) the possibility of crossing the collected information, either by the combination of private databases or by the use of sophisticated monitoring technologies;

(v) the necessity to control anonymity, in an attempt to draw the line between privacy and public safety, fighting crimes such as child pornography and counterfeiting;

(vi) the possibility of having citizens and customers under constant surveillance, through the dissemination of spyware bugs over the internet, such as worms.

These challenges, largely translated by the advent of sophisticated invasive technologies, made privacy in the cyberspace become a complex issue. From the moment that internet opens up ways for arbitrary use of monitoring technologies, not only by the state, but also – and especially – by the private sector, privacy is globally threatened.

It is high time to realize that Law is not the only means of fighting the new threats to privacy in the cyber era. People tend to believe in the myth that solutions come with new legislations. But legislations are slower than technology and there will always be a gap between them. In the digital age, technology can be the key to its own regulation. If the antidote is extracted from the poison and the vaccine is extracted from the virus, the same applies to technology. There shall be changes in the cyberspace's architecture in order to enable users to *actively control* the information that is collected about them. It is only when both the Law and Technology are combined that efficient solutions to protect privacy in a borderless territory can come up.

While it is still unclear which structure should be designed in order to enhance users' control over their information in the cyberspace, there is one thing that can be assured: having different and conflicting national legal concepts of privacy works for the disadvantage of the users, whose privacy rights are now dictated by private policymakers. They are the ones who make up their minds and set up the policies about what privacy should be. But they can change their minds. Anytime.