Personal data and Privacy protection

Publiee dans la revue de la faculte de droit.

Mona Al-Achkar

Professor of Law

Faculty of Law and Political Sciences- Filiere Francophone de Droit

maj_aj@hotmail.com

Mahmoud Jabbour

Professor of Political Sciences

Faculty of Law and Political Sciences- Section 2

Hannibal.m@hotmail.com

ABSTRACT

The growing use of mobile technology and the overgrowing opportunities to communicate, the internet of things, the clouding computer, make our personal data pour on the net, transform us into sensor for the world intelligence community[1], and blur the frontiers of legal sovereignty.

As a matter of fact, there is, next to the explosion of pouring data on the net, an explosion of mass communications surveillance guided by the commercial sectors, as well as, by nation states, and it is becoming very urgent to consider privacy protection in relation to personal data.

Actually, privacy protection laws have been introduced, in many countries around the world. Nevertheless, there is still a need to harmonize national legislation, to avoid hindering the free flow of personal data across frontiers, which may cause serious disruption in important financial sectors, such as banking and insurance.

Moreover, there is a need to balance upholding privacy as fundamental human rights, with other fundamental human rights such as free of expression and access to information.

Actually, Personal data illegal processing and use are making the headlines, and internet users' are becoming more aware about the dangers and risks of exposing their privacy, making protection of privacy as crucial in building confidence in cyberspace, and elemental in boosting innovation in digital economy, by ensuring e-transactions, e-government, and e-commerce.

Keywords: Personal data Protection; The right to Privacy;

1. Introduction

[1] P. Langlois- founder of the Paris-based company Priority One Security, on "agencies' ability to harvest personal data from users of smartphones." http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

While the use of network technology promises to bring information to the fingertips for those who need it, privacy concerns are increasingly rising.

Collecting personal data and abusing civil liberties are making the headlines in all kind of media, such as Snowden case, and WikiLeaks'one[2]. Recently, some governments are increasing their iron arm on Internet, by implementing measures to ensure user identification online[3].
Alternatively, Governments, as well as, the business community, are becoming more aware of consumers' privacy concerns, and have begun serious efforts at self-regulation. International organizations, public administration and businesses, embracing e-government and digital economy, show interest in ensuring that privacy is protected. Focus on privacy is getting more attention by many official and civil institutions, after realizing privacy's decisive role in building confidence in cyberspace by protecting consumer's rights and civil liberties.

2. Definitions

2.1 Personal data

While anonymity is not a recognized right, it is still a condition to protect privacy. In digital world, we are quickly moving from a world of anonymity to full identification and increased tracking of individuals' moves and behaves, through personal data collection, which drastically violates our right to privacy.

The Lebanese draft law issued by decree 9341 0n 8/10/2012 has adopted the common definition of personal information adopted in the OECD Privacy Principles[4] stating that it is any data that can lead to the identification of an individual, either alone or when combined with other identifying information.

Recently, the EU, trying to address the blurred lines around the protection of personal data, adopted a very specific definition of personal data In the General Data Protection Regulation's[5] declaring: it is any information relating to an individual, whether it relates to his or her private, professional or public life. Hence, personal data, could be anything, from a name, a photo, an email address, bank details, and posts on social networking, medical information, or a computer's IP address.

2.2 Privacy

According to U.S. Justice Louis Brandeis, the right to privacy is "the right to be left alone." Hence, personal information should be protected from public scrutiny. The Privacy means preventing

---

[2] "Attention fliers: Canada's electronic spy agency is following you - new Snowden" leaks.http://rt.com/news/canada-snowden-spying-nsa-airport-442/

[3] "China orders real name register for online video uploads." http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121

[4] OECD, *OECD Privacy Principles*, http://oecdprivacy.org/

[5] http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you

unauthorized disclosure of personal information held by the public sector administration, or by private professionals. It means also, prohibiting interference with one's personal life and affairs.

Hence, the right to privacy often means the right to personal autonomy, or the right to choose whether to engage in certain acts or have certain experiences. General principles of law recognize a general right for privacy, in any interaction with the society.

The close link between Personal data and the right of Privacy is so intense and very clear in the legislative context. Some new constitutions (South Africa) and Many European countries, have approved laws to regulate surveillance of personal data and protect citizens' privacy[6].

3. Mass surveillance

3.1 public sector

Cyber space represents the new dimension of national security. But traditional mission of monitoring and gathering information, by the Security forces, are not suitable enough anymore.
There is a need to identify, to target plotters and to anticipate the actions of networks that may be malicious and criminal.
Online surveillance is a new form of surveillance provided by new technologies. Governments are using far-reaching surveillance programs. Media have lately revealed scaring figures of commercial personal data, and streams of information skimmed from Smart phones' traffic, by security agencies, in many countries.
Most of the governments are using sophisticated technologies for monitoring computer networks and users, detecting intrusion, identifying and tracing intruders, and preserving and analyzing evidences: Tempora[7], SORM-2 and SORM-3, and social networks censorship[8].
Positive aspects of surveillance were evident. Tracking communications traffic, weaving together data from different sources and data mining Smartphone data, have been helpful in breaking up bomb plot by Al Qaeda in German in 2007, arresting of drug dealers[9], and dismantling child pornography network[10]. In this context, we can also mention some European research project, like The INDECT Project "Intelligent information system supporting observation, searching and detection for security of citizens in urban environment", which aims to ensure security of citizen, mainly against violence.

3.2 private sector

Corporations of all shapes and sizes, telecoms' providers, online advertising businesses and search engines, track our Internet activity and practice people profiling. The scale of collected data and

---

[6] FISA Amendments Act of 2008, Communications Assistance for Law Enforcement Act , in the USA

[7] Tempora, is a clandestine security electronic surveillance program tested in 2008, established in 2011 and operated by the British Government Communications Headquarters (GCHQ). http://en.wikipedia.org/wiki/Tempora

[8] G. King, J. Pan, and M. Roberts. "Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation", 2014. Copy at http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

[9] "Drug lord Guzman arrested." http://news.yahoo.com/internet-crucial-venezuela-battleground-075124059.html

[10] "How the NSA's High-Tech Surveillance Helped Europe Catch Terrorists" http://www.civilbeat.com/articles/2013/06/21/19341-how-the-nsas-high-tech-surveillance-helped-europe-catch-terrorists/

taped communications is quite remarkable, and represents a serious risk for privacy and civil liberties.
They compile personal data like age, sex and location, to send tailored ads to their mobile phones; they store and analyze data, and use them for commercial purposes. Sometimes, they collect particularly sensitive data, through what they called optional data; like ethnicity, marital status and sexual orientation.
Due to social media's atmosphere of "sharing," Individuals post their own personal information on social media networks, and share their status, photos, and geographic location.

Actually, two kinds of data are collected to identify individual behaviors' patterns. The first is from online communication platforms that allow internet users to join or create networks, and to voluntarily share personal information, opinions and common interests with other internet users. The second is metadata collected during users' activity: such as routing information, time stamps, and other data associated with calls collected by mobile devices.
According to secret British intelligence documents, spies are lurking in the background of popular games applications, to snatch data revealing the player's location, age, sex and other personal information[11].

3.3 The major customer of personal information: government

Next to their commercial use, collected data, could be swept up and mined by security agencies, for new information, to compare them with their lists of intelligence targets. Internet services represent a precious mine of information of interest, for the security agents. They allow locating the target when using Google maps, grabbing its friends and family lists of addresses, as well as the telephone logs, and the geographic data embedded in pictures sent to mobile versions of social networks.

4. Privacy

4.1 Users' expectations

Nevertheless, when individuals provide personal information, they expect two things: the first, that it would be used on the service for the sole purpose of providing the service requested.

The second: the respect of their desire to keep anonymous, a control on their personal data, and a discretion on part of the person to whom they deliver personal information.

Hence, individuals' information should not be used and disclosed for purposes beyond what the individual provided it for, and his expectation to be unidentifiable shall be respected. Nevertheless, online technologies are optimizing trailing, profiling, and targeting internet users.

4.2 Prejudicial Practices

The used techniques of making users agree on terms of contracts popped every then and now, as "terms of service agreement", covering the use and disclosure of personal information. These practices are undermining and abusing the freedom of contract and its principles such as: understanding, and

[11] L. Vaas "Spy agencies are slurping personal data from leaky mobile apps"- January 29, 2014- http://nakedsecurity.sophos.com/2014/01/29/spy-agencies-are-slurping-personal-data-from-leaky-mobile-apps/- consulted on 30/1/2014

manifestation of clear and free will in accepting some engagements and deciding liabilities. Moreover, some companies go so far, as to declare the provided information, as company "property."

On the other hand, Due to social media and an atmosphere of "sharing," the boundaries of personal privacy, as well as the definition of this right, are ever-changing. Individuals post their own personal information on social media networks, and share their status, photos, and geographic location.

Individuals are agreeing on policy of privacy, where they allow services providers share and use their personal data, as well as, their family and friends' ones within a group of companies, or with third parties:

- to receive offer services, content or advertisements
- for internal purposes such as data analytics and research to improve products, services and customer communications
- Data processing services, customer data management, evaluation of customer interest, customer research and surveys, Location data by service providers in the context of location-based products.

4.2.1 Unfair Clauses

we are witnessing the wide spreading of clauses, that violates the right of the consumer to be well informed, and the rise of a new unbalanced contract: a "contract of adhesion", where the will of the adherent, is reduced to none, and where the provider imposes his conditions. These clauses abuse the free will of the internet user. More dangerous, are the clause transferring the burden of data protection to the user himself, while the platform is the one who should bear this liability.

The Clauses integrated in the contract of agreement to be signed by the internet user, are abusive, because they clearly limit its right to bargain or to choose what he agreed on. They don't give him the possibility to object, or to provide a specific consent on particular issues, such as processing its sensitive data, or sharing data.

Most of the national legislations worldwide condemning abusive or unfair clauses, are fixed by regulation, and prohibited, especially when they are used against non-professional individuals, and the jurisprudence tends to interpret this prohibition in favor of the non-professional. In France, the consumer protection agency DGCCRF[12] issued a guidance on social media terms of use, considering that it constitutes an unfair clause, whenever it is written in a complicated manner that doesn't allow user to understand it, or when it misleads him, or prevents him from the protection of national law's provisions.

4.3 The right to privacy: international legal framework

The crucial importance of protecting Privacy, made it widely protected, since 1980, by states' laws, and more generally, thanks to the guidance of the model law from the OECD Privacy Guidelines of 1980[13], and the APEC Privacy Framework of 2004[14].

---

[12] http://www.hlmediacomms.com/2015/01/13/french-consumer-protection-board-cites-social-media-violations/

[13] OECD, *OECD guidelines on the protection of privacy and transborder flows of personal data*

[14] APEC, *APEC Privacy Framework*, (2004)

Almost every country in the world recognizes a constitutional right to privacy.

The UN has supported protection of privacy by backing up a draft resolution[15], prepared by Brazil and Germany, and titled "The right to privacy in the digital age"[16].

Nevertheless, despite the many efforts to protect communications online, the legal privacy protections stop at the border, and sensitive information could be captured through many technologies of tracking and collecting. That's why Europe has figured out the safe harbor agreement[17], and many efforts are still on way to ensure better protection cross-borders.

After starting the building of a true arsenal of legislatives and regulatory texts[18], EU is currently working on a draft regulation proposal titled: General Data Protection Regulation (GDPR), which is a part of Article 8 of the European Convention on Human Rights. It is due to come into effect in early 2015, and designed to unify and simplify data protection, across the 28 member countries of the EU. This regulation works on establishing an austere data protection compliance regime, with severe penalties of up to 100M euros, or up to five percent of worldwide turnover, for organizations in breach of its rules.

According to all mentioned legislations, a person has the right to determine what sort of information about him is collected and how that information is used. It has also the right to review his own personal information, ask for corrections, and be informed of any disclosures.

Nevertheless, privacy is still compromised, because the confidentiality is challenged by a legal framework that hinges protections on who maintains the information, how the network is structured, where data is stored, and how long it is kept.

5 Lebanon

5.1 current situation

In Lebanon, almost every institution dealing with personal files is collecting personal data, including sensitive data. This is true, not only for universities, schools, and hospitals, but also for the financial, commercial, economic and security sectors.

As a matter of fact, there is an exponential movement of collecting and processing personal data due to huge information systems, such as the ones used by the ministry of interior, the e-health, and the social

---

[15] UN, "General Assembly backs right to privacy in digital age", http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

[16] Sixty-eighth session- Third Committee- Agenda item 69 (b) Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

[17] https://safeharbor.export.gov/list.aspx

[18] Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data - Council of Europe, Explanatory Report to the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the Use of Personal Data in the Police Sector, European Convention for the Protection of Human Rights and Fundamental Freedoms, Charter of Fundamental Rights of the EU

security. Recently, the office of the minister of administrative development, suggested the implementation of the unique ID, in the context of its e-government strategy.

This project was rejected by the parliament commission in charge, because of the poor security techniques adopted in the creation of the ID's number, and that makes it easy to discover the identity of the concerned person.

5.2 Privacy Constitutional rights?

While not explicitly stated in the Lebanese Constitution, the right to privacy is protected through some provisions about human and civil rights.

The provisions of the Lebanese Constitution, could be used in varying degrees of success, in determining a right to personal autonomy, by doing, or abstain from doing, some actions.

The Lebanese constitution, promulgated in 1926 and amended many times till 1995, declare in its preamble, its respect for the covenants of the United Nations Organization, as well as for the Universal Declaration of Human Rights.

It protects the privacy of beliefs (art.9), the privacy of residence against illegal search (art.14), the liberty of individual against illegal or unreasonable searches, arrests or jail (art. 8), and the freedom of expression (art.13).

The Lebanese Penal law protects privacy, by recognizing the right of a suspect or an accused to keep silence, and to not disclose personal information, that might lead to self-incrimination.

Privacy is also protected in some statutory laws. The code of medical ethics[19] stating the obligation to protect person's health information. Article 579 of penal code enforce confidentiality on professional in general, and forbid divulgation, as well as the use of personal information, for personal benefit. Article 264 of civil procedures' code, enforce privacy by forbidding divulgation of personal information collected by lawyers and physicians. Bank secrecy system in Lebanon, ads to that, and makes people expectations of privacy protection increase.

In the marketplace, the protection consumer law enforces this right, through laws intended to prevent deceptive practices and unfair competition.

Financial institutions are also required to have safeguards that protect the information they collect from customers.

5.3 Telecom Data: Politics prevail

Despite the fact that the privacy of the Lebanese is protected in the constitution and international norms and charters, there are no guarantees the security services are not eavesdropping on the Lebanese, away from any legal oversight.

Various security services used the telecom data to pursue Israeli agents in the country, spy networks, and gangs were captured by intercepting and tracking calls, and so on. Accordingly, "The issue is dominated by political and intelligence-related considerations." The bad thing is, that these techniques

[19] Art 7 and 29 of Law 288, 22 Feb 1994 modified in 22 Oct 2012

have been publicized in the media, which alerted the criminals, who shall avoid using phones in their movements.

Few years ago, following attacks on citizens and political figures – such as bombing and armed clashes – the intelligence department, asked a permission to access telecom data. This created an intense controversy in the country, and the telecom ministry refused, because it violates the citizens' privacy.

Because of the controversy, a Lebanese delegation travelled to France, to closely examine France's experience in this regard. The delegation found out that France did not give the data to its security services except partially, in relation to a specific time and place, that the French prime minister, according to French norms, in such cases, would approach demands on case by case study, by obtaining the opinion of an independent judicial on the legality of each request, and its compatibility with the constitution and the citizens' privacy rights.

In Lebanon, Law 99/140 on eavesdropping, also requires an independent judicial panel to study any eavesdropping requests, by asking the opinion of an advisory judicial panel. This Law permits access to telecom data and interception of communications for a period "not exceeding two months". Article 16 restricts wiretapping powers to the Ministry of Interior. This law is based on a similar French law, which grants the finance minister similar powers as the defense and interior ministers in this regard.

Later, In March 2014, Telecommunications Minister Boutros Harb granted the security services full access to data. Three main political parties: Hezbollah, Free Patriotic Movement and Amal's ministers, objected on the grounds that Harb's decision was in breach of the personal freedom of citizens.

In order to stop the wave of political assassinations, 14 March, (the targeted party), has always show acceptance to access telecom data. Using telecom evidence in forensics investigations, before the Special Court for Lebanon, has unveiled the practice of surveillance within the Lebanese security services.

Finally, it is worth mentioning that, the Hizbullah, an armed faction, who has its own independent telecom infrastructure, accepted to give data specific to the area where a security incident had taken place or to a possible location of wanted suspects, upon request. Hezbullah arms put at risk, not only the privacy of its opponents, but their security as well.

It becomes clear that delivery of telecoms data partly or fully, depends primarily on the political affiliation of the minister of charge and the targeted party whether it is a rival or an ally.

6. The answer

In the wake of terrorism striking everywhere, mass surveillance, internet of things, cloud computing, e-innovation, disparity of legal systems, cross borders cooperation is the answer.

Therefore, the efficient answer seems the one that can cope with the international movements of our data on the net. A legislation that could balance the free flow of information, at national level, and cross borders, and the right to privacy looks crucial.

In this context, national government are invited to move toward cooperation, and benefiting from the already existing experiences, such the European one, which proved to be the most suitable to protect privacy and respect fundamental human rights, to provide a legal tool, that may address globalization

and developments in how we use, share and store data, how we protect it, to social networks and cloud computing, and how we secure transfer operations and respect the right to be forgotten.

7. Conclusion: reducing the risks

Protecting personal data aims mainly, to meet the challenges of using new technologies, in a global market, and actual massive surveillance practices. Its main objective is to ensure individuals' rights, in controlling the invasion of their privacy. Nevertheless, this cannot be done by ignoring the need to ensure a free flow of personal data, on national and international levels, neither without an effective implementation, clear rules, and a serious cooperation between different institutions, in public and private sectors.

There is a special need for dialogue between many professional and governments, concerned by ensuring the free flow of information as a pillar of the freedom of the internet, because, privacy on the internet requires a unique cooperation beyond national boundaries, as well as, a unique combination of tools: legal, technical, and policy.

Nevertheless, we are very aware that risks cannot be eliminated but reduced.