Computer Ethics - Philosophical Enquiry (CEPE) Proceedings

Volume 2019 *CEPE 2019: Risk & Cybersecurity* Article 9

5-29-2019

# Information Privacy: Not Just GDPR

Danilo Bruschi
*Università degli Studi di Milano*

# Information privacy: Not just GDPR

Danilo Bruschi
Università degli Studi di Milano

## Abstract

The "information rush" which is characterizing the current phase of the information age calls for actions aimed at enforcing the citizens' right to privacy. Since the entire information life-cycle (collection, manipulation, storing) is now carried out by digital technologies, most of such actions consists of the adoption of severe measures (both organizational and technological) aimed at improving the security of computer systems, as in the case of the EU General Data Protection Regulation. Usually, data processors which comply with these requirements are exempted by any other duty. Unfortunately recent trends in the computer attack field show that even the adoption of strongest cybersecurity protection measures cannot be enough for avoiding data breaches. Thus we must get used to the idea that due to a computer attack we can loose our privacy, and if the hacked system was compliant to law requirements we have no right to complain.

In this paper we argue that in all these cases measures have to be provided for supporting data breaches' victims. In this regard, we believe that a remedy based on the inspiring principles of the Fair Credit Billing Act can be a first step in the right direction.

*Keywords: Information Privacy, Cybersecurity, GDPR, Data Breaches*

## Introduction

A. Grove, one of the founder of Intel, during an interview (Growe, 2000), well described the effects that the information and communication technologies have on the right to privacy and that we are experimenting today:

> *Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age.*

An ever growing number of people now believe that the Right to Privacy as initially conceived (Brandeis & Warren, 1890) is unachievable in our hyper connected society. Internet itself, social network sites, email services, game, fitness, lifestyle and a myriad of other apps, wi-fi, social network plug-ins, smart watches and bracelets etc. are some examples of technologies which can be used to collect personal data and for individuals profiling. The problem is exacerbated by what is known as the privacy paradox: even if, when asked, individuals express their concerns about their privacy being infringed, they are still willing to give their personal details to online retailers as long as they had something to gain in return (Kokolakis, 2017).

In such a scenario it becomes really hard to enforce the right to privacy. The mainstream attitude is that of guaranteeing such a right by law, that is categorize the privacy violation as a crime and to impose to the subjects which hold, collect and manipulate personal data the adoption of good practices and technologies which reduces the risk of a data disclosure. Fine and penalties are introduced for punishing who carries such a crime and do not comply with legal requirements. On the other hand data processors which comply with the law requirements are exempted from any other duty (see for example GDPR art. 82 comma 2).

In this paper we argue that even if the cybersecurity community has made very significant progresses in the last 30 years, the computer systems are still vulnerable, even if well protected, as witnessed by the recent data breaches involving Facebook (Facebook Breach, 2018) and Google (Google Breach, 2018). In such a context a provision that exempts compliant data processors from any responsibility in case of a data breach, is very dangerous as it nurtures in the citizens a sense of distrust in the law as well as in the institutions responsible for enforcing the citizens' rights. We also point out that if so far the leakage of an individual's personal data was in somehow recoverable, the situation is going to change drastically with the availability on the net of genomic databases. Bank account numbers and passwords can be changed, physical or electronic documents (even public key certificates) can be replaced and old ones can be revoked. In contrast, a genome is not mutable nor revokable.

The solution to such a problem cannot be a further tightening of the regulations as it usually happens. We need to promote an alternative approach to the problem, which start from a basic principle: " Any individual whose personal data have been compromised, deserves unconditional compensation for the consequent losses (e.g. loss of credit or insurance, loss of reputation, loss of employment etc.). In this regard, we believe that a remedy based on the inspiring principles of the Fair Credit Billing Act (Billing Act, 1986) can be a first step in the right direction, at least until we will be able to guarantee that well protected systems are not vulnerable.

The rest of the paper is organized as follows. In section 2 we will provide elements for supporting the idea that the information rush is just at the beginning and future technological innovations will make it more aggressive. Subsequently we will provide an overview of the protection measures introduced by the GDPR for the protection of digital systems. In section 4 we will we briefly describe the most recent computer attacks, in order to provide the elements for assessing the adequacy of the protection measures adopted to protect computer systems. In section 5 we will summarize our main arguments and draw the consequent conclusions. Section 6 closes the paper.

## The Information Privacy Rush

In this section we briefly describe how the information technology contributed to exponentially increases, both from quality and quantity point of view, the availability of sources containing personal data, thus making it very attractive personal data infringements.

The first reported abuse of persona data dates back to 1890 in relation to the unauthorized distribution of some photographs:

> *For years there has been the feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspaper, long keenly felt, has been but recently discussed by an able write ..."* (Brandeis & Warren, 1890).

As technology progressed the number of recorded individual activities constantly increased as well the techniques for manipulating them. At present most of the data about individuals and all the activities that they undertake during their life are available. These data are collected by the many digital devices and apps that we are now using in everyday life: Internet itself, social network sites, email services, game, fitness, lifestyle and a myriad of other apps, wi-fi, social network plug-ins, smart watches and bracelets etc. Furthermore, with the spread of Social Networks people started to voluntarily share personal information which since then was really difficult, if not impossible to get. Individual started to post intimate photographs, sentimental information and feelings among other. Which is the real motivation behind such an attitude it is not clear yet (Kokolakis, 2017) we just limit ourselves in recording that individuals voluntarily contribute to increase the file of their personal records available on the net.

The last element we want to recall is related to genomic data. New businesses are growing in the net demanding DNA samples in change of some free services (see for example myheritage.com, 23andme.com, Ancestry.com). Such data is quite valuable as it provides information about genetic conditions and predispositions to specific diseases, cancer, or schizophrenia, information about ancestors, siblings, and progeny. Furthermore, it is hard to assess or estimate the extent of the personal information that could be extracted or derived from the genome in the future. (At the same time, it does not take a great leap of faith to believe that it will be impressive) (Ayday et. al. 2013).

All of the data described above are collected by a large number of data brokers which using data analytics algorithms can infer previously hidden information about data subjects. This means that individuals will never be able to know which of their personal information is known somewhere.

In conclusion, since the initial formulation of the right to privacy the scenario has significantly changed. The most significant changes are:

- the vast amount of personal data which now available on the net;
- the high quality of the data which can be collected, as in the case of genomic data;
- the possibility of inferring even more data than that directly collected;
- the increased commercial value of personal data.

All these elements contribute to make personal data a very valuable good and consequently to increase the number of people interested in trying to get access, in some way, to such data.

## GDPR Technical and Organizational Measures

In this section we briefly review, from a technical point of view, the approach adopted by the GDPR for the protection of personal data. The most important GDPR articles which refer to practical measures which personal data processors have to adopt in the process of collecting, processing and storing personal data are: article 5 which declares the principles which have to be adopted, and article 32 which defines the main properties which such measures have to satisfy, more precisely, it is stated:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.*

It turns out that the GDPR does not provide any specific detail about such measures, besides requiring them to be appropriate to deal with an estimated level of risk computed on the basis of various factors such as: the state of the art, the costs of implementation, the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

On the other it is not difficult to identify in these propositions the solicitation for the adoption of a risk based cybersercurity approach as promoted by the International Organization for Standardization (ISO) through the ISO 27000 family of standard . ISO/IEC 27001 is one of the most popular and commonly used information security standards, and countless organizations have certified against it for the purpose of demonstrating adequate security to customers, business partners and regulators. In (ISO Report, 2018) it is reported that, as today, 68% of organizations are using ISO/IEC 27001 to achieve GDPR compliance.

ISO/IEC 27001 requires organizations to establish, maintain and continually improve what is defined an ISMS (Information Security Management System). We briefly recall that an information security management system (ISMS) is an organization's systematic approach to managing and protecting the confidentiality, integrity and availability (CIA) of information. More specifically, an ISMS includes the policies, procedures, guidelines, technologies, activities and controls employed in pursuit of that aim. Implementing ISO 27001 requires a comprehensive, well-planned and well-executed project.

Fine and penalties are introduced for punishing who does not comply with legal requirements. Organizations will be audited by a data protection authority (DPA), who will determine whether or not they are in compliance with the spirit of the regulation, discouraging organizations from focusing on finding loopholes. Consumers can bring complaints directly to the DPA as well. The penalties range from a warning to a fine up to 20m or 4% of their annual turnover, whichever is greater, per offense.

In conclusion, the GDPR promotes the adoption of the most recent cybersecurity standards and best practices. Since we are in a transition phase the adoption of such measures is far from be completely adopted by most businesses as it requires investments and an high level of competences, and many businesses involved in the transition process report budgetary problems, as well as a lack of appropriate skills.

## Recent Trends in Computer Attacks

In this section we provide a brief overview of the most recent computer attacks which appeared in literature, in order to assess the adequacy of the measures adopted to protect personal data with respect to most advanced form of computer attacks.

Since the eighties cybersecurity issues have taken on a prominent role in any organization and today they represent a day-to-day struggle for businesses. We briefly recall that a computer attack is often perpetrated by exploiting a vulnerability which is found in some software component, being it an application or some operating system element, or some configuration error. All IT vulnerabilities result from human error.

Since the beginning the research community has tried to counteract such a phenomenon, but it has been unable to keep the pace with the exponential growth of ICT technologies and consequently the number of software components placed on the market. Increasingly, everything is becoming a computer: not just our laptop and phone, but our car, our appliances, our medical devices, etc. On any of such devices we have software products and applications, and consequently a huge number of vulnerabilities is every day brought into the network.

The situation today is so critical that according to the World Economic Forum's Global Risks Report 2018 (WEF Report, 2019), the threat of cyber-attacks sits just behind extreme weather events and natural disasters in terms of events likely to cause disruption in the next five years. As a witness of such a situation we remind that the largest collection of breached data in history has been recently discovered. It comprises more than 770m email addresses and passwords posted to a popular hacking forum in mid-December (Hern, 2019).

Obviously not all vulnerabilities have the same penetration power, many of them only allow a limited number of unauthorized activities on the attacked system, on the other hand many other of them can be used for subverting a system overcoming every type of protection in place. This is the kind of vulnerability we want to get the reader's attention on as they are not rare and a stronger form of this type of vulnerability had been recently discovered, trough two computer attacks, namely Spectre and Meltdown (Kocher et. al., 2018; Lipp et. al. 2018). They represent a new class of attacks as they exploit hardware vulnerabilities, not software ones. Usually a standard vulnerability affect a specific system, that is the system which hosts the vulnerable application (eg. Windows vulnerabilities do not affect Linux systems and vice versa). Spectre and Meltdown attacks instead can be used for exploiting any platform as they exploit hardware bugs not software bugs. Patching them requires large-scale coordination across the industry, and sometimes patching isn't possible; the vulnerability will remain until the computer is discarded. They're the future of security and it doesn't look good for the defenders. They affect virtually all high-end microprocessors produced in the last 20 years. As mentioned in the paper abstract:

> *This paper describes practical attacks that combine methodology from side channel attacks, fault attacks, and return-oriented programming that can read arbitrary memory from the victim's process. More broadly, the paper shows that speculative execution implementations violate the security assumptions underpinning numerous software security mechanisms, including operating system process separation, static analysis, just-in-time (JIT) compilation, and countermeasures to cache timing/side-channel attacks. These attacks represent a serious threat to actual systems, since vulnerable speculative execution capabilities are found in microprocessors from Intel, AMD, and ARM that are used in billions of devices*.

This means that potentially today almost all of the protection measures adopted for increasing the security of a system can be subverted and, from our point of view, this requires a rethinking of the strategies, which are adopted for protecting personal data stored on computer systems, or equivalently, for protecting the right to privacy in our era.

## Not Just GDPR

In the previous section it has been shown that research in cybersecurity has revealed the presence of attacks that are able to violate the content of a system no matter what kind of protections has been adopted. This means that not only we have to get used to the idea of an increasing number of data breaches but, most importantly such data breaches will occur on well protected systems. Such a fact is usually sufficient to prejudice the right of individuals to lodge a complaint of an alleged infringement of their personal data, or better to get a compensation for the suffered damage. As an example of such a situation we report comma 1 and 2 of art. 82 of the GDPR, which clearly states what above mentioned:

> *Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller*.

That is, in a near future there will be individuals whose right to privacy has been violated by a computer attack, but they will not be able to take action against such a violation, because the processors of their personal data were compliant with the law. In these cases the obligation for the notification of a personal data breach to the supervisory authority and to the data subject has been introduced (GDPR art. 33 and 34) but we believe that being notified of a data breach is not enough, or better is no more enough.

If so far the leakage of an individual's personal data was in somehow recoverable, the situation is going to change drastically with the collection and availability of genomic data. For example, bank account numbers and passwords can be changed, physical or electronic documents (even public key certificates) can be replaced and old ones can be revoked. In contrast, a genome is not mutable nor revokable. Moreover, as large portions of it are passed on to future generations, disclosure of one's genomic information can turn into an endless curse for both current and future generations.

In order to deal with such an issue the legislator has, from our point of view, two possible choices. Either, further strengthen the protection measures just adopted till to prohibit the collection of particular types of personal information, or starting from the realistic assumption that both technology and law are not perfect, assume the existence of people who will loose their right to privacy and elaborate a different approach for at least compensating their consequent losses.

We believe that the first approach cannot bring significant results, it is well known that there will never exist completely secure systems as well as that we have inadequate legislative instruments to deal with complexity and pervasiveness of cyberspace. In this sense we are still going through a transition phase whose end is difficult to see: "most laws were conceived in and for a world of atoms not bits" (Negroponte, 1996).

The second approach may instead be more promising. In this case a program has to be individuated in order to help people which are victims of a personal data breach, to recover to their normal life. Thus overcoming some consequences such as the loss of employment, credit or insurance as well as the loss of reputation they may suffer because of the leakage of personal data.

In this context it could be worth to take inspiration from the principles underneath the Fair Credit Billing Act. A federal law enacted to protect consumers from unfair billing practices, such as unauthorized charges, charges for unaccepted or undelivered goods and services and other disputed charges. In all these case consumer is liable for $50 for unauthorized use of a credit card. In our specific case we need to protect consumer from unfair use of personal data stored by some data processors. When this happens, no matter why and how, the data processor has to contribute to repair the consequences of personal data breach.

A further alternative which could be considered is that of introducing a form of social welfare programs. These governmental programs are usually designed to protect citizens from the economic risks and insecurities of life. In our specific case the risk to be protected against is determined by the discrimination which can derive once your personal data has been revealed, and the condition for requesting a compensation are not satisfied. The level of benefits will depend on the severity of damages suffered. The program could be financed by organizations involved in the Big Data business.

## Conclusions

The existence of regulations such as the GDPR are very important as they try to put a stop to the spread of illegal practices of collecting and manipulating personal data, and punish all the abuses. On the other provisions have to be introduced for dealing with cases which are not “covered” by the law. In such cases the solutions have to be found in different contexts. In the previous section we have proposed two approaches which can be used for individuating such solution and which are based on the assumption that a State should not only be focused on guaranteeing to its citizens the recognition and the enjoyment of the right to privacy but it should also be involved in supporting them when such a right is violated, as in the case of some other important rights such as: job, home and health.

## References

Ayday, E., De Cristofaro, E., Hubaux, J.P., Tsudik, G., (2013), The Chills and Thrills of whole Genome Sequencing. Retrieved from http://infoscience.ep.ch/record/186866.

Billing Act. (1986). Retrieved from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-billing-act

Brandeis, L., Warren., S. (1890). The right to privacy. *4 Harward Law Review*, 193.

Facebook Breach. (2018 September). Retrieved from https://newsroom.fb.com/news/2018/09/security-update/.

GDPR. (2016). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj..

Gove, A. (2000). What I've learned . *Esquire Magazine*, May.

Hern, A. (2019). Largest collection ever of breached data found. Retrieved from https://www.theguardian.com/technology/2019/jan/17/breached-data-largest-collection-ever-seen-email-password-hacking

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, *Computers & Security* (Vol. 64, pp 122-134).

Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., Yarom, Y. (2018). Spectre Attacks: Exploiting Speculative Execution . Retrieved from http://arxiv.org/abs/1801.01203

ISO Report. (2018). Retrieved from: https://www.itgovernance.co.uk/iso27001-global-report-2018

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., Hamburg, M. (2018) .Meltdown. Retrieved from http://arxiv.org/abs/1801.01207

Mac Millan, D., Mc Millan, R. (2018 October). Google Exposed User Data, Feared Repercussions of Disclosing to Public. Retrieved from https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194

Negroponte, N. (1996). *Being Digital*. New York: First Vintage Books Edition.

Purtova, N. (2015). The illusion of personal data as no one's property. *Law Innovation and Technology* (vol. 7 pp 83-111).

Watcher, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, (Vol 34 pp 439-449).

WEF Report. (2019). Retrieved from: https://www.weforum.org/reports/the-global-risks-report-2019.