Accepted Manuscript

Contemporary technology management practices for facilitating social regulation and surveillance

Rodrigo Martínez-Béjar, Gaspar Brändle

PII: S0160-791X(17)30116-1

DOI: 10.1016/j.techsoc.2018.04.003

Reference: TIS 1052

To appear in: *Technology in Society*

Received Date: 27 April 2017

Revised Date: 16 April 2018

Accepted Date: 23 April 2018

Please cite this article as: Martínez-Béjar R, Brändle G, Contemporary technology management practices for facilitating social regulation and surveillance, *Technology in Society* (2018), doi: 10.1016/j.techsoc.2018.04.003.

Contemporary Technology Management Practices for Facilitating Social Regulation and Surveillance

Rodrigo Martínez-Béjar
E-mail: rodrigo@um.es
Department of Information Engineering and Communications
Faculty of Information Technology
Campus Universitario de Espinardo
University of Murcia
30100 Spain

Gaspar Brändle
E-mail: gbrandle@um.es
Department of Sociology
Faculty of Economics
Campus Universitario de Espinardo
University of Murcia
30100 Spain

Address correspondence to:
Gaspar Brändle
E-mail: gbrandle@um.es
Department of Sociology
Faculty of Economics
Campus Universitario de Espinardo
University of Murcia
30100 Spain

Contemporary Technology Management Practices for Facilitating Social Regulation and Surveillance

Abstract

The opportunities provided by new technologies signify that current societies have an unlimited number of possibilities as regards improving the quality of their citizens' lives. Governments and some corporations may simultaneously use such technologies to achieve some of their goals with a greater effectiveness than before. However, the usages that governments and corporations make of these technologies could lead to an institutionalisation of practices that may be questionable. These practices embrace the access and use of confidential or private information by governments, in addition to corporative practices that may violate some fundamental liberties when corporations act as government collaborators.

The goal of this research is to describe some of the most recent socially-relevant social control and surveillance practices carried out by governments, along with the irregular personal information management practices of corporations, through the use of Information and Communication Technologies in the European Union and North American regions. The research data have been taken from (academic, media, civil society and corporative) publications available from the beginning of the 2000s to the present. The findings show a wide variety of practices (e. g., mass surveillance or the violation of personal information privacy), which appear to be more institutionalised in North America, and particularly in the United States, than anywhere else in the European Union or Canada.

Key words

Social control; Surveillance; Privacy; ICTs, Biometrics

Introduction

Individuals from advanced societies are subject to observation, scanning, digitisation, etc., by the authorities in order to facilitate recognition and identification and, ultimately, to achieve a minimum level of social control. To this end, the authorities use new generation technologies to implement several practices. Perhaps one of the most recent and illustrative examples of the usefulness of such surveillance by the security forces is the central role played by the data obtained, primarily as result of these practices, in the resolution of the bomb attack at the Boston Marathon in 2013. However, events such as the cases of Edward Snowden or Julian Assange show that there have also been illegal practices within the framework of the surveillance to which our society is subject.

Without questioning the efficacy of new technologies as regards solving complex social and economic problems, one may wonder whether our societies have any limits by which to control our privacy. Authorities and large corporations have frequently invoked security against terrorism and improving individuals' quality of life as arguments to justify surveillance and the spread of biometric controls. However, the vast majority of society ignores the nature of the personal information that, as citizens or users of contemporary technologies, people put into the hands of authorities and large corporations.

For example, almost every time we use the Internet to connect to a service or use an app, we click on to accept a document that contains a large number of conditions and terms of use without being aware of what exactly we are accepting (Palfrey and Zittrain, 2011). And we very often do this because of the desire to communicate with others (Turkle, 2011). As Boyd (2013) puts forward, the default options could be a risk for users because those options convey information sharing. In other words, there is always a risk for Internet service users that their private information may be made publicly available by these services. In addition to this, default settings vary over time, and this could cause problems for users if they do not review the changes made.

Furthermore, all the transactions implied in these uses, such as those made by means of whatsapps, chats, messages, tweets, information searches, commercial transactions, etc., leave a digital trace with some personal information that is stored in large databases and files in which it is possible to identify us (Tufekci, 2014). 'Globalisation' also takes place more and more frequently with our data (Vaidhyanathan, 2011). This is in line with the claims put forward by Lippert and

Newell (2016), who also state that attention should be paid to the fact that the business models of large Internet companies, such as Facebook and Google, involve the very efficient collection of users' data. This has immensely facilitated the tasks of security agencies.

According to Décary-Hétu, Morselli and Leman-Langlois (2012), the problem is that there would appear to be evidence that the majority of people do not have any inconvenience as regards sharing their personal information, and there is no noticeably significant social reaction against the notable increase in surveillance or a generalised corporate demand to control personal information regarding private lives.

Furthermore, it has become evident that biometric technologies are being increasingly applied and deployed in real settings, signifying that all that is characteristic of humans (e.g., faces, fingerprints, etc.) is currently a source of information. One example of this is the fact that devices equipped with cameras (e.g., smart phones, tablets, etc.) are able to recognise users' faces. In general terms, it can be assumed that if a citizen is honest, the role of Information and Communication Technologies (ICTs) may well be limited to making her/his life more comfortable. However, there do not appear to be sufficient institutional debates regarding the limitations and scope of contemporary ICTs and information privacy. This, according to the proposals put forward by Husserl, leads to the risk of conceiving humans as things (San Martín, 1987). To be more precise, it can be said that there is, for example, a commercial objectification of our faces in that we become clients from the moment we are identified by a biometric device and we could be recognised at any time without our consent. As Décary-Hétu *et al*. (2012) have pointed out, the potential presence of biometry in our everyday environments such as our office, home, mobile terminals, etc., therefore, seems unavoidable. This raises doubts as to whether it is reasonable to accept biometry in all these environments.

In this context, it is worth asking what the impact of ICTs and biometric systems on society is. The problem to be addressed in this research is accordingly related to the new forms of social control and management of personal information carried out by the political and economic powers. We shall, therefore, investigate how some governments make use of contemporary ICTs to, supposedly, improve their citizens' security, when it could eventually be a method by which to increase social control. We shall also investigate the links between the free availability of access to Internet services (apps, social media, etc.) offered by large corporations, the default settings using by such

services and, principally, the management of users' information that is made by those corporations. Some research has, to date, addressed certain relevant aspects of governmental social regulation practices in countries like the USA (Palfrey and Sohoian, 2014), Ireland (Schneier, 2015), France and Spain (Lippert and Newell, 2016) without specifying any pre-defined temporal study. Likewise, it is possible to find some literature dealing with irregular personal information management policies and practices recently carried out by specific companies (Ramonet, 2010; Vaidhyanathan, 2011; Schneier, 2015). The purpose of the research presented herein is to fill in the gap we have found in the literature concerning the identification and categorisation of common social regulation or privacy management practices carried out by governments and corporations, respectively, during the period 2001-2016 in North America and the European Union.

1. Social control in historical perspective

The problem of social control has been subject to research since Sociology first appeared as a discipline. In fact, the term social control originally alluded to the societal ability for self-regulation, although during the 1930s, the term started to be conceived predominantly as individual conversion to conformity (Roodenburg, 2004). Some other authors have been responsible for the existence of two different control approaches since the 1960s. One is that of North America, which emphasizes the social processes involved in the construction of consensus and conformity. The other is that of European, which focuses on the juridical and institutional expressions of the State (Horwitz, 1990).

According to the arguments of Janowitz (1975), the concept of social control is closely related to social order, and takes place in the institutions of several modern societies, including those constituting the pillars of the welfare state (e.g., the inspection of people receiving social services or subsides), the productive system (e.g., the surveillance of employees' activities or of users of certain services), politics (e.g., the follow-up of voters' opinions by means of societal research) or the educative system (e.g., the design of university degree curricula). In a dialectics between elite and social collectives, some researchers have indicated the relevance of transparency in the interaction process as an effective instrument by which to avoid conflict (Sumner, 2012).

Another interesting contribution is made by Harvey (2010), who has emphasised the need for a historical analysis of the social control process. This author is responsible

for the shift that this process has undergone from the deliberative democracy perspective, whose values are continually being redefined and negotiated through interaction, to the that of the unquestionable imposition of a normative consensus, thus leaving little margin for the plurality of viewpoints.

It has been argued that these perspectives have since led the term social to be understood as a conscious process with a number of functions, including those of: giving a meaning to and shaping our way of thinking and being; provoking and monitoring social acts and identities; and causing the prosecution of the dissident up to the individual itself (Edwards, 1988; Sumner, 2012).

This vision contrasts with what has been put forward by other sociologists, who have argued that the new urban exclusion processes are the origin of an increase in violence and crime, apart from turning the social control down (Sampson, 2012). Other authors have attempted to draw a map of the probability of certain collectives committing crimes, theorising that it is more probable that individuals or collectives who are not sensitive to the social consequences of their crimes will commit them (Bushman *et al*., 2016). These authors have assumed that conformist individual conduct is a function of the existent links between the individual and the social groups to which they belong. If these links are sufficiently strong, that is, if they involve a high degree of identification with conventional processes and objectives, adherence to forms of authority or the sharing of socially accepted beliefs, then conformist behaviour will predominate.

Gottfredson (2013) has argued that the transfer of the concept of social control is based on the relationship among social agents and the concept of self-control. He states that this type of self-control, which can be acquired during the first stage of infancy, may be understood as the individual ability to regulate her/his own conduct in terms of planning her/his acts, the postponement of her/his satisfaction, and cohabitation with frustration.

There is also abundant literature concerning the effects of control on a whole society, sometimes referred to as societies of control (Deleuze, 1992) or the disciplinary society (Ewald, 1989), for whom the central idea is that society, in that disciplinary state, creates a type of common language for all kinds of institutions. This disciplinary society refers to the generation of an exchangeable, continuum space (Foucault, 1975). For this latter author, disciplines are the language of contemporary societies, signifying that corporal training practices are generalised through three processes. Firstly, there is

a mutation in the conception of discipline, which goes from a blocking technique to an effective mechanism with which to make individuals useful. Secondly, there is a certain amount of liberation of disciplines, signifying that the discipline is seen as instrumental for general welfare. Thirdly, a centralised police emerges with the purpose of practicing de facto global surveillance in order to make the whole social body visible.

Literature has also paid attention to the role of specific techniques and technologies as tools by which to govern conducts. Thus, according to Rose (1997), the concept of normality arose in the context of a social concern about ways of thinking, conduct or expression that were considered negative or dangerous.

The panoptical theories, which are very popular in social sciences, have their fundamentals in Bentham's architectonic planning for disciplinary institutions. The ultimate objective of this architectonic model was to achieve continuum, omnipresent, horizontal and hierarchised individual monitoring, for which purpose a tower was designed from which guards could monitor individuals while being invisible to the individuals being monitored. More generally, Deleuze (1992) has stated that the Panoptical model may be understood as a group of functions and regularities shared by disciplinary institutions. With regard to self-control, the development of the panoptical control techniques gave rise to a feeling of constant surveillance that causes each individual to exert self-control and conform blindly to the rule (Foucault, 1975).

1.1.ICTs as means of social control and surveillance

New technologies have served as an impulse to the application of panoptical theories in current western societies. Thus, the panoptical model has been extrapolated into ICT-based surveillance. Consequently, electronic panopticon (Robins and Webster, 1999) has been often thought as an effective, powerful surveillance system in terms of all speed, coverage, accuracy or size, so that ICTs advances will make it possible that the whole society is subject to surveillance (Marx, 2002).

From another perspective, Poster (1995) has introduced the term 'super-panopticon', pointing out that databases allow panoptic principles to function as a super-panopticon, which is a more general panopticon operating at the level of the whole of society rather than being limited to particular institutions, as is the case of the classic panopticon. In addition, this author believes that the super-panopticon is more discrete and less efficient as regards normalisation than is a classic panopticon. Moreover, Lyon (2001) stated that citizens actively contribute to the operation of the

super-panopticon since they provide it with the information required for their own surveillance as part of their daily life.

Other terminologies introduced around the concept of the panopticon include the virtual or cybernetic panopticon (Whitaker, 1998) and the Techno-panopticon (King, 2001), which refer to the panopticon that has arisen from the application of digital technologies specifically or new technologies in general.

It has been claimed elsewhere that there has been a transition from classic institutional control to control carried out by surveillance agencies, which are constituted by a convergence of old and new discrete surveillance mechanisms. This has led to the proliferation of automated socio-technical environments (Lianos and Douglas, 2000). Furthermore, individuals are tempted to obtain certain social or economic benefits from the Internet (e.g., by accessing particular services), but this usually only occurs if they can be monitored by ICT-based surveillance systems (Haggerty and Ericson, 2000).

The characterisation of control in the so-called Information Society has been subject to research by Robins and Webster (1999), who have pointed out that this kind of society is more controllable, monitorable, and transparent. In other words, in the opinion of these authors, the Information Society is more disciplined. Their investigations complement others, such as that described in Gandy (1996), whose main claim is that in western societies, personal information forms part of an economic logic in a panoptical schema.

The usage of ICTs in the surveillance of urban spaces has also received a considerable amount of attention recently. The increasing number of surveillance systems in streets, on public transport, etc., has led some social research works specialised in urban areas to transform or adopt the panoptic perspective. For McCahill and Norris (2002) and Koskela (2003), the deployment of those systems can be understood as a complex and advanced extension of the panopticon, thus allowing the constant surveillance of moving individuals. In addition, according to Fyfe and Bunnister (1996), surveillance cameras make it possible to create anticipatory conformity habits, since the individuals being observed interiorise surveillance as something ubiquitous.

Other authors have highlighted that surveillance video cameras in urban public spaces, unlike traditional disciplinary techniques, solely allow a superficial image of the individual to be obtained (Jones, 2000). In their research on surveillance in urban

spaces, Graham and Wood (2003) have put forward the theory that digital surveillance techniques make it possible to translate space into a controllable language. From another analytic perspective, Koskela (2003) has argued that surveillance is founded on the need to clean the public space of everything that can be an obstacle to consumption in such spaces. This theory connects with the vision described by Davis (1990), for whom security is a relative value as a function of economic possibilities. This in some respects coincides with the theory of Bauman (1998), who points out that the concept of public space understood as a collective space has disappeared, apart from the fact that there is a real investment in the public sphere by private interests seeking to promote consumption.

2. Method

This research is focused on investigating the nature and scope of (1) detected social regulation practices carried out by governments and (2) corporative actions that have to do with potential violations of ICT users' privacy rights. The geographic area researched was North America (i.e. the USA and Canada) and the European Union, while the period of study was 2001 - 2016. The research should be put in the context of an attempt to shed more light on how the new paradigm regarding social surveillance that arose as a consequence September 11th 2001 is working.

The specific research objectives we pursued are the following:

In relation to governments, our goal was to detect and categorise governmental practices reported in the mass media, academic publications or relevant Internet-accessible contents, that have to do with the use of ICTs for social regulation.

With regard to corporations, our objective was to identify and categorise the practices of some corporations as reported in the mass media, academic publications or relevant Internet-accessible contents as regards the use of ICTs to irregularly manage personal information.

These research objectives were then used as a basis on which to establish several hypotheses for the above mentioned geographic and temporal scope, with the purpose of discovering (1) whether the reported targeted governmental/corporative kinds of practices are isolated from one another; and (2) whether these practices are extended in geographic terms. If so, it would be apparent that, at least in the European Union and North America, these kinds of practices are becoming institutionalised.

With regard to reported governmental practices related to social regulation, the hypotheses tested are shown below.

- H1: There are a variety of reported governmental practices involving the use of ICTs that have to do with social regulation during the period in question.
- H2: The same kinds of reported practices involving the use of ICTs that have to do with social regulation can be found in several countries of the two geographic areas subject to research during the period in question.

With regard to reported corporative practices related to irregular/questionable personal information management, the hypotheses tested are indicated as follows.

- H3: There are a variety of reported corporative practices involving the use of ICTs that have to do with irregular/questionable personal information management during the period in question.
- H4: The same kinds of reported practices involving the use of ICTs that have to do with irregular/questionable information management can be found in several companies in the two geographic areas subject to research during the period in question.

In relation to data collection, we used the following procedure. First, academic publications were obtained by carrying out a literature review through the use of standardised tools employed in academic literature searches, such as Google academic and indexed academic databases available at our Institution. Publications in prestigious mass media were then selected by using a web browser, along with terms alluding to the meaningful research topics, such as ‘privacy’, ‘social control’ or ‘electronic surveillance’. Finally, those web portals that were relevant to our research were selected as data sources for our research upon the allusion of the corresponding institution (i.e. company, government or non-profit organisation) or web portals in some (academic or mass media) publications selected for this research.

The institutions/web portals selected as data sources were: AT&T, Credit Info, Electronic Frontier Foundation, Facebook, Google, Government of Canada, AOL, Internet Archive, LinkedIn,Mashable, Ministère de l’intérieur (France), Wikileaks, and Wired. In addition to that, the following media were used to search for relevant data: Daily Mail & General Trust, Dow Jones & Company, Guardian Media Group, Nash Holding (Bloomberg), NBC Universal Media, The New York Times, Time Warner, Tribune Company, and US News & World Reports.

The field work lasted for approximately one year, from February 2016 to March 2017.

The content analysis methodology was subsequently used to analyse the data (i.e. texts) collected as described above. The data analysis process took 1 about one month and was carried out using the Atlas.ti software toolkit (version 7). The main aim was to find and describe a number of specific cases of both (1) the most socially-relevant, contemporary ICT-supported practices as regards social control and surveillance carried out by governments and (2) ICT-supported personal information mismanagement by corporations in the period referred to above. In this respect, it is worth pointing out that the corpus of analysis did not aspire to be statistically representative, since there was no valid sampling frame for all the reported policies and actions carried out by the governments and corporations in the regions and period under study and from which that representative body of information could be extracted. However, the selection sought to be exhaustive, following a systematic procedure as regards searching gor and selecting information that would allow an accurate description of the phenomenon under study.

3. Governmental mass surveillance practices involving Information and Communication Technologies

3.1.Internet technologies-based mass surveillance

In January 2002, the USA Defense Advanced Research Project Agency (DARPA) initiated the so-called 'Total Information Awareness' (TIA) project, whose mission was to register all kinds of digital transmissions (Tribune Company, 2002). As Lyon (2014) has stated, the intention of this project was actually to link users' online activities to searches for flights or financial transactions. The rational for this project was the US authorities' belief that they might be able to predict whether a crime was going to be committed if they had sufficient data. But the TIA was officially cancelled being rejected by the US Congress owing to the controversy that it generated. However, the George W. Bush government decided to keep the project alive in an illegal, secret manner. Moreover, president Obama did not cancel the communication-monitoring programme once his presidency began (Electronic Frontier Foundation, 2016b).

One of the major massive scandals to have occurred recently concerns what is denominated as the 'Massive interception' software programme, created by an espionage network formed of several western countries (Dow Jones & Company, 2012).

This programme processed citizens' communications in order to extract information patterns. This programme affected the citizens of several countries included in this investigation, as reflected below in Table 1, which also contains information regarding some activities that were carried out by that programme. Moreover, in order to save all the data collected by the National Security Agency (NSA) through the massive surveillance of the Internet, this organisation has built a huge data centre whose cost exceeded 1 billion US$ (Wired, 2014).

Insert Table 1 about here

The aforementioned network was also used to organise access-restricted fairs. The presence of governmental agencies together with technology supplier companies, many of which were included in the Wikileaks files (Wikileaks, 2014) was usual at these fairs. Furthermore, the USA government has also encouraged software developers to improve the tools required for the massive surveillance of Internet activities, and several large corporations have developed this type of software (Mashable, 2012). This has been fruitful up to the point that, according to Wikileaks' latest revelations, the CIA used top-of-the-range software tools during the period 2013-2016 in order to break into the most common devices connected to the Internet. In particular, all smartphones, computers and even Internet-connected televisions have been used as devices to collect multimedia (i.e. voice, video and textual) information from at least USA citizens (The New York Times, 2017).

Moreover, as has been pointed out by Pell and Soghoian (2014), the typical customers of massive surveillance technology vendor companies are other companies, such as telecommunication operators and Internet providers, along with governments. According to these authors, the commitment to spy on their own users or clients is commonly imposed on customer companies. Likewise, according to these authors, all information flowing through the Internet or mobile devices, such as smart mobile phones, is monitored by means of the devices supplied by these vendor companies. Large Internet corporations and governments, therefore, have huge amounts of data from their citizens at their disposal. Moreover, these companies and governments have argued that such data are useful to prevent individuals from carrying out a certain action or to detect anomalies (Time Warner, 2013).

According to Palfrey and Zittrain (2011), there is a legal emptiness regarding digital environments in the USA and, under the so-called 'third-party doctrine', it has, therefore, been assumed that an individual who voluntarily facilitates information to

third parties must not expect her/his privacy to be maintained. In practical terms, this means that if a consumer shares her/his data with a company, the right to be legally protected in relation to the privacy of those data comes to its end (Pell and Soghoian, 2014). In addition, it is much more efficient for a government to ask companies for personal data rather than obtaining these data by using traditional governmental practices, such as listening to phone calls. This signifies that, if the government receives news that a third party has carried out a particular information collection task about an individual, the government benefits from that third party rather than having to do the task itself (Palfrey and Zittrain, 2011). In fact, the principal technological corporations receive thousands of requests concerning information delivery about those corporations' users or clients from the US federal government (Pell and Soghoian, 2014).

Moreover, from the mid 1980s on, there has been a legal figure for the regulation of governmental demands in the USA whose goal is to reveal the contents electronic communications, such as e-mails, saved in computer systems. It is, therefore, feasible for the US government to request data regarding an individual's location without mediating any judicial approval (Calo, 2012). In 2010, the FBI consequently made various requests to several Internet companies with the purpose of investigating certain individuals linked to the Wikileaks issue (Lyon, 2014).

Regulations concerning digital content and privacy have also been violated in the European Union (EU), where companies are obliged by law to supply their users with all the data they have about the latter. As has been described in Scheneier (2015), the social activist and ex-Facebook user Max Schrems, together with other activists of the 'Europe vs. Facebook' movement, have consequently been involved in a judicial battle with the Irish government from the year 2008. More precisely, and based on the above-mentioned EU regulations, he has been unsuccessfully requesting that the Irish government apply the aforementioned regulations with regard to Facebook, whose main European headquarters is located in Dublin.

From the year 2002, there have been several preventive detentions in USA as a result of the massive surveillance of the Internet. Victims of these detentions have included non-USA citizens and minors (Daily Mail & General Trust, 2011a). This has led to the situation in which, in 2012, a few days after a young Irish man wrote a humorous tweet saying that he would destroy America during his planned holidays in the USA, he was arrested upon his arrival in the USA and kept in jail for a few hours after his interrogation (Athavale, 2012). Preventive detentions have also been reported

outside US territory. In the UK, it was discovered that protests were going to occur thanks to the surveillance carried out. Moreover, some famous activists who were going to participate in those protests were prevented from attending them (Guardian Media Group, 2011a).

Many of the practices described above have been published in the mass media, and have sometimes had considerable consequences for particular journalists. During the Obama presidency, after government agencies had spied on numerous journalists, a number of federal complaints were, therefore, submitted against the majority of the journalists who denounced bad governmental practices, amounting to a greater number than those submitted during the entire history of the USA before the Obama presidency (US News & World Reports, 2013).

In other countries, such as Spain, there has been another kind of mass surveillance, which has had important consequences in terms of privacy. In particular, from the beginning of the 2000s, the Spanish government has implemented a security policy consisting of installing video cameras in the suburbs with the highest reported crimes rates. These cameras record real time videos whose contents are also analysed in real time by dozens of members of the security forces located in several control centres. The purpose of this policy is crime prevention, in addition to ensuring an effective reaction should crimes be committed in the area under video surveillance (Ramonet, 2010).

3.2.Biometric technologies-based mass surveillance

Another kind of ICT-based surveillance promoted and implemented by some governments is that of biometric systems. In this respect, the Canadian government has funded and developed the Nexus project, which was ideated to accelerate the transit across the USA-Canada border (Government of Canada, 2014). With this project, Canada intends to make use of the iris as a personal identifier, thus enabling air travellers to cross the aforementioned border very rapidly. It is sufficient to look at a camera, which is designed to carry out iris recognition, and the authority allows the transit of those individuals whose irises have been recognised.

The Nexus project was developed in collaboration with the US government and has several general objectives. Firstly, this project aims to make it easier for ‘low risk’ individuals tocross the USA-Canada border. Secondly, it also seeks to decongest the terrestrial border offices of both countries at peak times. All of this allows those people

who have pre-registered with the Nexus system to cross the border in an easier and faster manner than those who do not make use of that system. This may by the reason why the majority of Nexus users are in favour of setting up Nexus (Desenne and Jourdain, 2012). Moreover, borders on which Nexus has been applied allow customs officers to primarily focus on risk citizens.

In 2007, the French government and Paris airports started to develop the Parafe system, which is also based on biometric technology (Ministère de l'Interieur, 2012). The purpose of this system is to modernise and accelerate transit across French borders, such that all 'honest' citizens can cross them as rapidly and securely as possible. Parafe, which requires for a previous registration, does this by taking fingerprints from eight fingers.

3.3.Summary of governmental mass surveillance practices

As has been put forward previously, one of the main objectives of this work was to shed some light on the most relevant institutionalised ICT-supported governmental practices that have to do with social regulation. In an attempt to summarise the data presented above, Table 2 includes the following information:

- Practice, namely, a brief sentence describing the detected practice.
- Publication. This refers to the nature of the publication(s) in which the researchers found information about the governmental practices analysed.
- Government, that is, the government involved in the practice in question.
- Collective, which refers to the kind of social collective(s) affected by the practice.
- Technology, which provides information concerning the kinds of technologies amongst those targeted in this research that have been used for surveillance purposes.

Insert Table 2 about here

3.4.Data analysis of reported governmental mass surveillance practices

According to the data above, it follows that the US government is involved as a major player in most of the categories of practices detected. The publications describing some of the practices targeted in this research generally stem from Academia. The presence of the civil society, normally through NGO channels, and the mass media as another relevant source of information, and which are active denouncers of the practices in question, are also noteworthy. Most of the collectives affected by governmental

social regulation practices meet the condition of being ICT users. Finally, Internet technologies are mainly employed to achieve governmental objectives in the context of social regulation, although some biometrical systems-based practices have also been detected.

In summary, the following findings related to the reported categories of relevant practices carried out by at least one government within the geographic area under study can be highlighted:

1. Mass surveillance, which plays some of the following roles: active participation, direction, government's coordination, research and development or investment in large technological infrastructures to improve mass surveillance.
2. The control of people's movements, including terrestrial border control, preventive detentions and video surveillance.
3. The registration of all kinds of digital transmissions.
4. Corporative services users and clients being hindered access to their data by the corporations that provide these services.
5. The revelation of electronic communications without requiring the authorities' prior approval by introducing new regulations.
6. Court acts against denouncers of bad governmental practices.

Both hypotheses H1 and H2 can, therefore, be said to hold in our geographical and temporal space. Moreover, all of these findings can be interpreted as evidence of Foucault's proposals (see Foucault, 1975) when he argued that contemporary societies will tend to carry out practices involving a de facto global surveillance with the purpose of making the entire social body visible. We have consequently found that several western societies have, during the years since the beginning of this century reported that it is more and more common for their respective governments to carry out this kind of practices in a number of manners, which are common to several societies, at least in the geopolitical area studied in this research. These manners include: mass surveillance, the control of citizens' movements, the registration of citizens' digital transmissions, not supporting citizens' aspirations to discover their data registered by corporations, irregular revelations of citizens' electronic communications and the promotion of legal actions against complainants of such practices.

These findings would also appear to support the theory described in Ramonet (2010), which is focused on the apparent institutionalisation of mass surveillance practices carried out by some governments in the European Union.

4. Corporate ICT-based practices involving citizens' private information

Companies, in particular those offering Internet social network-like services, have strong economic incentives to both maintain as much of their users' information as possible and make it as shareable as is technically feasible (Tufekci, 2014). However, from the psychosocial point of view, it is well known that, in the context of human relations, it is not usually good for one person to know everything about what another person has done, said or written (Turkle, 2011). One of the reasons for this last assertion is, in line with what has already been pointed out elsewhere (Calo, 2012), that companies can make use of the information they have about a person in a way that could have negative effects on that individual.

One of the most extended corporative practices amongst those detected in this research is the participation of corporations in the global massive surveillance network in cooperation with certain governments, as published by Wikileaks. In particular, these companies have provided security agencies with their respective users' information without letting the latter know about the provision of that information. The majority of these enterprises belong to the ICT sector, and many of them are quite well-known, as is the case of Apple, AVM Software –the developer of the Paltalk service-, Facebook, Google, Microsoft, Skype, which was recently acquired by Microsoft, Yahoo, and Youtube, which is currently owned by Google. But companies pertaining to other sectors, along with those belonging to the mass media (e.g., CNN, Fox News, MSNBC –currently owned by NBC), the financial sector (e.g., Mastercard, PayPal Holdings, Visa), telecom operators (e.g., AOL before being purchasing by Verizon Communications), commerce (e.g., Amazon), among others (Wired, 2011; Nash Holding, 2013), have also been found to be involved in these activities.

4.1.ICT corporations

One of the most surprising practices detected in various ICT corporations, such as Facebook and Twitter, is that consisting of carrying out the mass surveillance of users on the basis of their Internet activities (Mashable, 2012). On other occasions, there seem to be clear privacy violations. Another aspect of interest concerning privacy issues

is the report published by the Electronic Frontier Foundation (2016a), according to which several large corporations have had an important influence on policy makers, which has originated from the pressure that some companies put on politicians to favour those corporations' interests within the context of US privacy legislation. For instance, the Facebook, Google and Twitter corporations managed to achieve that a law proposed by a Senator protecting children's and adults' privacy on the Internet was not approved by the California Senate in 2011 (Tribune Company, 2011).

The information that the Facebook Corporation has about its users embraces many different types of specific data concerning a number of facets of their daily life. These data may be easily found in pdf documents by typing words like 'party' or 'sex' in such a way that each user's relevant facets, including those related to their political leanings, psychology or hobbies, may be inferred from these documents (Scheneier, 2015). This signifies that even if a user of the Facebook service has used this for a short amount of time, Facebook will have a data file for that user which is much larger than that which any security agency may have about the same user. In addition, if a user clicks on the Facebook delete button in order to remove information, this will, nevertheless, be kept by Facebook. Furthermore, some researchers have found evidence that Facebook actively collaborates with governmental security agencies (Pell and Soghoian, 2014), and these researchers have stated that this company has dozens of employees whose sole occupation is user surveillance.

LinkedIn, prior to its purchase by Microsoft in June 2016, set up its polemic service acceptation conditions stipulating that LinkedIn corporation permanently owned the information uploaded by users (Linkedin, 2016). The Pinterest platform was also surrounded by controversy in 2012 because its terms of use included the fact that this corporation was the owner of the user contents uploaded onto that platform (Monoyios, 2012). Once these terms of service were published early in 2012, the scandal was such that the corporation announced that from April 2012 onwards the term 'property' would disappear from the clauses contained in its terms of use (Mellow, 2012).

The privacy policy of Google Corporation has evolved since that first established at the end of the 1990s as will be noticed in Google (2016a). According to the oldest privacy norms set up by this company on its web site (Google, 2016b) in January 4th 2001, user data can be revealed. Nevertheless, according to the privacy policy published before this date (Internet Archive, 1999), user data are anonymous. It is, therefore, possible to state that Google has omitted the information regarding the

oldest privacy policies from its web site for some reason. Moreover, the privacy policies management of this corporation may lead one to believe that there are no guarantees that the use of the Google search engine is really free. In addition, in January 2012 Google announced that it would modify its privacy norms (The New York Times, 2012a). To be more precise, Google proceeded to combine the personal information collected by its services and to save this information in a single profile (Time Warner, 2012). This new norm was published on March 1st 2012 (Google, 2016c).

4.2.Telecom operators

According to one of the clauses included in the AT&T privacy policy, this company will 'assist in the prevention and investigation of illegal activities and violations of our Terms of Service or Acceptable Use Policies' (AT&T, 2016). In this sentence, attention is drawn to the usage of the word 'prevention'. Furthermore, an ex-employee of AT&T showed sensitive documents to a Non-government organisation, and the information contained in those documents demonstrated that this company collaborated in an active fashion in a programme whose goal was to listen to telephone calls (Electronic Frontier Foundation, 2016c).

4.3.Commerce corporations

In 2012, an article appeared in The New York Times (2012b) concerning a man, who apparently felt offended, causing trouble in a Target-owned shop in Minneapolis, USA because Target was sending unrequested information to his underage daughter. Moreover, the information, which was based on her Internet shopping habits that this corporation somehow knew, was useful only for pregnant women. However, the aforementioned man, who did not know that his daughter was pregnant, thought that Target was inducing his daughter to get pregnant.

4.4.Financial entities

In the year 2008, thousands of American Express clients underwent a significant reduction in their credit limits with no prior notification. When these clients noticed this reduction, they contacted the financial entity in question, and this entity then explained that these clients had shopped shortly before the reduction in the same places as its defaulting clients (Credit Info, 2008).

4.5.Mass media

In 2006, AOL published its users' browsing history once these were made anonymous, that is, after substituting its users' identity information for codes (AOL, 2006). However, only a few hours after, a huge controversy arose because a journalist discovered the identity of one particular user after analysing these browsing history profiles (The New York Times, 2006).

In the year 2011, the UK society was shocked when a newspaper published information concerning a female teenager who had been murdered in 2002. Apparently, according to the data registered on her mobile phone, someone had listened to and removed information from her mobile phone after the date on which she was supposed to have been murdered. This publication led her family to believe that she might have been alive at the time of those mobile operations. However, what had in fact happened was that the News Corporation's employees, with the help of some UK police officers, had tapped the mobile phone with the purpose of obtaining the first news about her case (Guardian Media Group, 2011b).

4.6.Summary of ICT-supported corporative practices related to privacy management

As has been stated previously, one of the objectives of this work was to discover more about the most controversial ICT-supported corporative practices that have to do with privacy management. Table 3 summarises the data collected as regards the management practices described above.

Insert Table 3 about here

4.7.Data analysis of reported ICT-supported corporative practices related to privacy management

A brief analysis of the data in the table above allows us to underline that almost all of the corporations identified are based in the USA. The mass media has been the most common source of information, followed by the civil society, by means of Non-Governmental Organizations or individuals, and finally academia and corporate web portals. The vast majority of the companies identified that have carried out mismanagement regarding personal information and that may have been involved in privacy violations are from the technological sector. Finally, the social collectives most

affected by the corporative users' privacy management practices are the users/clients of such corporations.

In summary, the following findings related to reported relevant practices carried out by several companies can be highlighted:

1. Violation of the right to personal information privacy through the use of practices such as:
    a. Unconsented publication of users or clients' data.
    b. Non-communication of information supply of users or clients' personal data to governmental agencies.
    c. Unconsented publication of users' browsing/information search histories.
    d. Establishment of privacy policies with clauses stipulating cooperation with the corresponding government for illegal actions prevention.
    e. Participation in phone taps realised in the context of governmental programmes.
    f. Delivery of all information written on smart mobile phones to governments.
    g. Free disposal of users' data for other users without their prior consent.
    h. Successful actions, such as lobbying governments with the purpose of promoting corporation-favourable regulations concerning information privacy management.
2. Reduction of available financial credit with no previous warning to the users affected by this reduction.
3. Surveillance of Internet services users' activities.
4. Sale of private data to governments.

Both hypotheses H3 and H4 can, therefore, be said to hold in our geographical and temporal space. Furthermore, these findings seem to validate, at least in part, Tufekci`s theory (see Tufekci, 2014) in that more and more corporations in several western countries retain and manipulate the data we supply to them in order to identify us and take the corresponding actions, such as reducing our credit (in the case of financial entities), selling our data or monitoring our Internet activity. Moreover, our findings regarding the widespread reported multiple corporative practices that violate the right to personal information privacy might, to some extent, support Vaidhyanathan (2011), who claims that there is more and more globalisation of our data.

These findings are also in line with that put forward by Boyd (2013), in that there is a real risk for all Internet service users that their personal information may be made publicly available by these services. Finally, our findings seem to reinforce the theory of Bauman (1998), who argues that modern societies can be characterised by a real investment in the public sphere by private interests seeking to promote consumption.

5. Conclusion

The current technological civilization is founded on technical systems that are capable of a number of tasks, including organising, managing and controlling fluxes (goods, information, and people). For example, the biometric cards given to individuals registered in biometric systems in the context of projects such as those described above, make it possible to manage fluxes of people crossing a border. It can consequently be stated that this type of projects constitutes a good example of an ICT-based manager model that characterizes contemporary technological societies.

In view of the data obtained in this research, it can be highlighted that the governmental and corporative control of citizenship on the basis of ICT activity is a clear reality in today's western civilisation. More precisely, this control is more and more extensive in western societies that are highly linked to ICTs in a growing number of everyday life facets. In this respect, and in accordance with that stated by an ex NSA agent, all communications carried out electronically by US citizens have been spied on (NBC Universal Media, 2009). Moreover, in line with Turkle (2011), citizenship can be said to have favoured this espionage because of the citizens' desire to make all aspects of human life more comfortable by using ICTs as much as possible. However, in this research it has become clear that numerous instances of academia, prestigious mass media, corporations and civil organisations (mainly NGOs) have stated, either directly or by publishing information, their position against the contemporary ICT-based highly sophisticated control to which western societies are subject de facto.

Taking into account the capacity and the scope of the practices carried out by massive global surveillance networks, it can be affirmed that if something is digitalised, then it is not really a private issue. In other words, it could be admitted that the digital alter ego of each individual is totally controlled. In this respect, citizens' capacity to react is very limited if we assume that governments know all the relevant aspects of those citizens who use intelligent smart mobile phones or the Internet, that is, virtually everyone.

It is also worth noting that the results from this research are consistent with the more general theory contained in Castells (2006, 2009) in the sense that there is some collaboration among the elite members of the technology, communication, politics and economy sectors as regards facilitating an effective social control in our society. Furthermore, all this takes place within a context characterised by highly intensive globalisation and technological revolution processes accelerated by the use of Internet technologies and their associated services.

In relation to biometric technologies, it is usually assumed that the greater the number of security technologies, the more protection citizens receive (Magnet and Mason, 2014). In this respect, it can be said that the latest generation of passports are quite secure, because they contain a very sophisticated identification system for signatures. More precisely, these passports include some sort of hologram, apart from other integrated technologies and a picture. Taking this into account, it might be asserted that it is not necessary to add more security technologies to passports. In fact, the current proliferation of biometric technologies seems to be a result of artificial necessities created in order to justify corporate strategies rather than a social demand.

In general terms, a certain social concern with regard to the deployment of biometric systems has become apparent. In addition, there is some fear regarding a number of issues that cause social controversy, such as attacks targeting personal data or the use of personal data files with a different purpose to that which is authorised. Similarly, security restrictions are increasing in such a way that the search for infallible systems is providing promising results and thus opening up new opportunities (and market) for corporations to do business.

It would appear that citizens are becoming accustomed to new ICTs, and to the Internet and biometric technologies in particular. More precisely, it has become apparent that more and more human functions are delegated to ICT-based systems. This leads to a situation in which citizens are unable to discover many details as regards problem solving, but only whether or not something fires an alarm, works, accepts, and so on. This phenomenon may lead to a loss of part of the social attitude as regards confronting new challenges, including conflictive situations in terms of all moral values, interests, etc.

A social paradox might be taking place. On the one hand, the social acceptability of new ICTs implies the social requisite of respect for privacy by governments and corporations, something that is apparently not occurring in western societies in a

number of specific situations reported in this research. On the other hand, the users' acceptance of these technologies conveys the achievement of minimal user effort, such as being identified by the authorities when crossing borders.

Citizens should prompt their politicians and governments to force security agencies to operate in another manner in relation to the management of personal information based on the misuse of contemporary ICTs. In this respect, in the USA there is still no effective norm regulating practices allowing corporations and governmental agencies to protect citizens from the mismanagement of personal data. Moreover, all this occurred during the Obama presidency and despite his own declarations against these kinds of abuses before becoming president of the USA (Obamaspeeches, 2009).

However, in the EU context, there are some good examples of the fulfilment of citizens' demands for digital privacy. In particular, the French institutional system for citizens' rights in relation to ICTs can be highlighted. This system represents a paradigmatic case of institutional citizens' protection against possible abuses regarding privacy violations involving ICTs in that two institutions play an important role (Ramonet, 2010). Furthermore, there is an agency, named CNIL, which is in charge of monitoring this freedom, and some of its main functions are those of authorising and creating binding reports concerning the acceptability of new technologies in addition to the data or information that these technologies handle or save. Thus, given a new technology, CNIL forbids its deployment until the entity in charge of exploiting that technology has received the corresponding CNIL authorisation for the new technology to be put into routine use.

In the future, we shall carry out research into the apparent fact that the majority of people do not have problems as regards sharing their personal information without really knowing the consequences that that sharing may imply. We shall additionally investigate whether, as we believe, there does not yet seem to be a significant, coordinated and strong social reaction against the notable increase in surveillance, biometric controls or personal information revealed through the irregular management of ICTs. Finally, we plan to shift our focus from the descriptive perspective taken in this work to an explicative one by exploring a number of facets involved in theoretical works, if any, or the testing of hypotheses claiming institutional, conscious ICT-supported personal information mismanagement by some of the most popular ICTs and companies. In line with this, we will carry out a variety of case studies regarding the

privacy policies undertaken by these companies in order to attempt to test these theories/hypotheses.

References

AOL. (2006). AOL proudly releases massive amounts of private data (online). Retrieved 10 March 2016, from http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/

Athavale, Chandrashekhar. (2012). A costly tweet (online). Retrieved 14 March 2016, from http://www.akshardhool.com/2012/06/costly-tweet.html

AT&T. (2016). AT&T privacy policy (online). Retrieved 10 March 2016, from http://www.att.com/gen/privacy-policy?pid=2506

Bauman, Zygmunt. (1998). *Globalization: The human consequences*. Columbia University: Press.

Boyd, Danah. (2013). Networked privacy. *Surveillance & Society, 10*(3/4): 348-350.

Bushman, Brad, Newman, K., Calvert, S.L., Downey G., Dredze, M., Gottfredson, M. et al. (2016). Youth violence: What we know and what we need to know. *American Psychologist, 71*(1): 17-39.

Calo, M. Ryan. (2012). Against notice skepticism in privacy (and Elsewhere). *Notre Dame L. Rev.* 87: 1027-72.

Castells, Manuel. (2006). *La sociedad red*. [The Network society] Madrid: Alianza Editorial.

Castells, Manuel. (2009). *Comunicación y poder*. [Communication and power] Madrid: Alianza Editorial.

Credit Info. (2008). AmEx reducing credit limits based on what you buy, where you live (online). Retrieved 5 April 2016, from http://www.creditinfocenter.com/wordpress/2008/10/09/amex-lowering-credit-limits/

Daily Mail & General Trust. (2011a). War on… teenagers: Boy, 13, interrogated by the SECRET SERVICE for posting message about Bin Laden on Facebook (online). Retrieved 16 March 2016, from http://www.dailymail.co.uk/news/article-1388087/Vito-LaPinta-13-interrogated-SECRET-SERVICE-Osama-Bin-Laden-Facebook-post.html

Daily Mail & General Trust. (2011b). Now TomTom apologises for selling customer satnav data...which police used to set up speed traps (online). Retrieved 16 March 2016, from http://www.dailymail.co.uk/sciencetech/article-1381491/TomTom-apologise-selling-customer-satnav-data-used-police-speed-traps.html

Davis, Mike. (1990). *City of quartz: excavating the future in Los Angeles*. London: Verso Books.

Décary-Hétu, David, Carlo Morselli and Stephane Leman-Langlois. (2012). Welcome to the scene: a study of social organization and recognition among warez hackers. *Journal of Research in Crime and Delinquency*, *49* (3): 359 - 382.

Deleuze, Gilles. (1992). Postscript on the societies of control, *October*, *59*: 3-7.

Desenne, Patrice and Bernard Jourdain. (2012). Fenêtre sur corps (online). Retrieved 28 February 2016, from https://www.youtube.com/watch?v=1WJPyww3UOQ

Dow Jones & Company. (2012). The surveillance catalog-where governments get their tools (online). Retrieved 14 March 2017, from http://graphics.wsj.com/surveillance-catalog/

Edwards, Anne R. (1988). *Regulation and repression: the study of social control*. Sydney: Alien & Unwin.

Electronic Frontier Foundation. (2016a). The privacy shield is riddled with surveillance holes (online). Retrieved 11 March 2016, from https://www.eff.org/es/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes

Electronic Frontier Foundation. (2016b). NSA Spying on Americans (online). Retrieved 11 March 2016, from https://www.eff.org/es/nsa-spying

Electronic Frontier Foundation. (2016c). Public unredacted klein declaration (online). Retrieved 11 March 2016, from https://www.eff.org/es/document/public-unredacted-klein-declaration

Ewald, François. (1989). Um pouvoir sans dehors [The power without outside], In *Michel Foucault philosophe. Rencontre internationale Paris 9, 10, 11 janvier 1988*. Paris: Éditions de Seuil.

Foucault, Michel. (1975). *Surveiller et punir: Naissance de la prison* [Discipline and Punish: The Birth of the Prison] Paris: Editions Gallimard.

Fyfe, Nicholas R, and Jon Bannister. (1996). City watching: closed circuit television in public spaces. *Area, 28*(1): 37-46.

Gandy, Oscar H. (1996). Coming to terms with the panopticon sort, In David Lyon and Elia Zureik, (Eds.), *Surveillance, Computers and Privacy* (pp. 132-155). Minneapolis: University of Minnesota Press.

Government of Canada. (2014). Nexus (online). Retrieved 2 March 2016, from http://www.cbsa-asfc.gc.ca/prog/nexus/

Google. (2016a). Actualizaciones política de privacidad [Privacy policy update] (online). Retrieved 10 March 2016, from https://www.google.es/intl/es/policies/privacy/archive/

Google. (2016b). Política de privacidad [Privacy policy] (online). Retrieved 10 March 2016, from https://www.google.es/intl/es/policies/privacy/archive/20010104/

Google. (2016c). Condiciones de servicio de Google [Service terms and conditions] (online). Retrieved 10 March 2016, from https://www.google.com/policies/terms/archive/20120301/

Gottfredson, Michael R. (2013). A note on the role of basic theory in thinking about crime prevention. *European Journal of Crime Policy and Research, 19*: 91.

Graham, Stephen and David Wood. (2003). Digitizing surveillance: Categorisation, space and inequality. *Critical Social Policy, 23*(2): 227–248.

Guardian Media Group. (2011a). Royal wedding protest: three anti-capitalist activists arrested (online). Retrieved 1 April 2016, from http://www.theguardian.com/uk/2011/apr/28/royal-wedding-protest-three-arrested

Guardian Media Group. (2011b). Missing Milly Dowler's voicemail was hacked by News of the World (online). Retrieved 1 April 2016, from http://www.theguardian.com/uk/2011/jul/04/milly-dowler-voicemail-hacked-news-of-world

Haggerty, Kevin and Richard Ericson. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4): 605-622.

Harvey, David. (2010). *The enigma of capital and the crises of capitalism*. London: Profile Books.

Horwitz, Allan V. (1990). *The logic of social control*. Nueva York: Plenum press.

Internet Archive. (1999). Google and cookies (online). Retrieved 5 February 2017, from https://web.archive.org/web/19991012225420/http://google.com/privacy.html

Janowitz, Morris. (1975). Sociological Theory and Social Control. *American Journal of Sociology, 81* (1): 82-108.

Jones, Richard. (2000). Digital rule: Punishment, control and technology. *Punishment and Society, 2*(1): 5-22.

King, Lyall. (2001). Information, Society and the Panopticon. *The Western Journal of Graduate Research, 10*(1): 40-50.

Koskela, Hille. (2003). 'Cam Era': The Contemporary Urban Panopticon. *Surveillance and Society, 1*(3): 292-313.

Lianos, Michalis and Mary Douglas. (2000). Dangerization and the end of deviance: The institutional environment. *British Journal of Criminology, 40*(2): 261-278.

LinkedIn. (2016). Terms and conditions (online). Retrieved 1 February 2017, from https://www.linkedin.com/legal/user-agreement?trk=hb_ft_userag

Lippert, Randy K and Bryce Clayton Newell. (2016). Debate introduction: the privacy and surveillance implications of police body cameras. *Surveillance & Society, 14*(1): 113-116.

Lyon, David. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, David. (2014). Surveillance, Snowden, and Big Data, capacities, consequences, critique. *Big Data & Society, 1*(2): 1-13.

Magnet, Shoshana and Corinne Lysandra Mason. (2014). Of trojan horses and terrorist representations: mom bombs, cross-dressing terrorists, and other queer orientalisms. *Canadian Journal of Communication, 39*(2): 9-26.

Marx, Gary T. (2002). What's New about the 'new surveillance'? classifying for change and continuity. *Surveillance & Society, 1*(1), 9-29.

Mashable. (2012). Revealed: The FBI Wants to Monitor Social Media (online). Retrieved 7 February 2017, from http://mashable.com/2012/01/26/fbi-social-media-monitoring/#jTXNR821WaqZ

McCahill, Michael and Clive A. Norris. (2002). Literature review (Working Paper No.2). On the threshold to urban panopticon? Analysing the employment of CCTV, In *European Cities and Assessing its Social and Political Impacts* (pp. 1-18). Berlin: Centre for Criminology and Criminal Justice.

Mellow, Glendon. (2012). Pinterest updates Terms of Service, drops the 'sell'. *Scientific American*, March 24.

Ministère de l'intérieur. (2012). Parafe (online). Retrieved 5 February 2017, from http://www.parafe.gouv.fr/

Monoyios, Kalliopi. (2012). Pinterest's terms of service, word by terrifying word. *Scientific American*, March 19.

Nash Holding. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program (online). Retrieved 9 February 2017, from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

NBCUniversal Media. (2009). Keith Olbermann interviews Russell Tice - NSA Wistleblower - on Countdown (online). Retrieved 5 January 2017, from https://www.youtube.com/watch?v=vqigfE0nBs0

Obamaspeeches. (2009). Floor Statement General Michael Hayden Nomination (online). Retrieved 5 February 2017, from http://obamaspeeches.com/073-General-Michael-Hayden-Nomination-Obama-Speech.htm

Palfrey, John G and Jonathan Zittrain. (2011). Better Data for a Better Internet *Science, 334* (6060): 1210-1211.

Pell, Stephanie K and Christopher Soghoian. (2014). Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy. *Harvard Journal of Law and Technology, 28*(1): Fall 2014.

Poster, Mark. (1995). *The Second Media Age*. Cambridge: Polity Press.

Ramonet, Ignacio. (2010). Pensamiento único y nuevos amos del mundo [Unique thinking and new masters of the world], In Noam Chomsky e Ignacio Ramonet (eds.), *Cómo nos venden la moto. Información, poder y concentración de medios* [Information, power and media concentration]. Barcelona: Icaria.

Robins, Kevin and Frank Webster. (1999). *Times of the technoculture. From the information society to the virtual life*. London: Routledge.

Roodenburg, Herman. (2004). *Social Control in Europe I: 1500-1800*. Ohio: University Press.

Rose, Charles. (1997). Electronic Monitoring of Offenders: A New Dimension in Community Sentencing or a Needless Diversion? *International Review of Law, Computers, and Technology, 11*(1): 147-154.

Sampson, Robert J. (2012). When things aren't what they seem: context and cognition in appearance-based regulation. *Harvard Law Review Forum, 125*: 977-107.

San Martín, Javier. (1987). *La fenomenología de husserl como utopía de la razón*. Barcelona: Anthropos.

Sumner, Colin. (2012). Censure, culture and political economy: beyond the death of deviance debate, In Steve Hall [ed.], *New directions in criminological theory*, Cullompton: Devon.

The New York Times. (2006). A face is exposed for AOL searcher No. 4417749 (online). Retrieved 1 March 2017, from http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&

The New York Times. (2012a). Google to Update Privacy Policy to Cover Wider Data Use (online). Retrieved 1 March 2017, from http://bits.blogs.nytimes.com/2012/01/24/google-to-update-its-privacy-policies-and-terms-of-service/?_r=0

The New York Times. (2012b). How Companies Learn Your Secrets (online). Retrieved 1 March 2017, from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&hp=&pagewanted=all

The New York Times. (2017). WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents (online). Retrieved 1 March 2017, from https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html?_r=0

Time Warner. (2012). Google to merge user data across its services (online). Retrieved 15 June 2016, from http://edition.cnn.com/2012/01/24/tech/web/google-privacy-policy/

Time Warner. (2013). Why I'm quitting Facebook (online). Retrieved 15 June 2016, from http://edition.cnn.com/2013/02/25/opinion/rushkoff-why-im-quitting-facebook

Tribune Company. (2002). George Bush's Big Brother (online). Retrieved 7 April 2016, from http://articles.latimes.com/2002/nov/17/opinion/oe-turley17

Tribune Company. (2011). Online privacy bill fails to pass California Senate (online). Retrieved 7 April 2016, from http://articles.latimes.com/2011/may/28/local/la-me-social-networking-20110528

Tufekci, Zeynep. (2014). Engineering the public: Big Data, surveillance and computational Politics. *First Monday, 19*(7).

Turkle, Sherry. (2011). *Alone together: why we expect more from technology and less from each other*. New York: Basic Books.

US News & World Reports. (2013). Obama Talks a Conciliatory Tone About News Leaks- The president responds to criticism administration is targeting journalists (online). Retrieved 11 March 2017, from http://www.usnews.com/news/blogs/ken-walshs-washington/2013/05/24/obama-talks-a-conciliatory-tone-about-news-leaks

Vaidhyanathan, Siva. (2011). *The googlization of everything and why we should worry*. Berkeley: University of California Press.

Whitaker, Reginald. (1998). *The end of privacy: how total surveillance is becoming a reality*. New York: New Press.

Wikileaks. (2014). The Spy Files (online). Retrieved 8 March 2016, from https://wikileaks.org/the-spyfiles.html

Wired. (2011). Twitter's response to WikiLeaks subpoena should be industry standard (online). Retrieved 8 April 2016, from http://www.wired.co.uk/news/archive/2011-01/11/twitter-subpoena-reaction

Wired. (2014). Edward Snowden: The Untold Story (online). Retrieved 8 April 2016, from http://www.wired.com/2014/08/edward-snowden/

Table 1. **Activities and countries subject to massive espionage**

Massive espionage activity	**Affected countries**
Internet monitoring	Canada, USA; UK, France, Italy, Holland, Germany, Hungary, Poland, Sweden
Phone monitoring	Canada, USA; UK, France, Italy, Holland, Germany, Hungary, Poland, Sweden, Czech Republic.
Troyans	Germany, UK, France, Italy
Speech analysis	USA, Spain, UK, France, Italy, Germany, Czech Republic, Belgium, Denmark.

Source: Wikileaks (2014).

Table 2. Governmental ICT-based social control practices

Practice	Publication	Government	Collective	Technology
Participation in massive surveillance network.	Wikileaks (2014)	Canada	Phone and Internet users	Internet
		UK		
		USA		
Human control in borders.	Desenne and Jourdain (2012)	Canada	'Low risk' Canadian citizens transiting to USA by road	Biometry
		USA	'Low risk' USA citizens transiting to USA by road	
Registration of all kinds of digital transmissions.	Electronic Frontier Foundation (2016b)	USA	Phone and Internet users	Internet
Application of the 'third-party doctrine'.	Palfrey and Zittrain (2011)	USA	USA users of services companies	
Unauthorized revelations of electronic communications.	Pell and Soghoian (2014)	USA	Individuals and NGOs involved in Wikileaks	
Support to software tools development for Internet-based massive surveillance .	Mashable (2012)		Internet services users	
Erroneous massive surveillance-based detentions.	Daily Mail Trust & General Trust (2011a)		USA citizens, Foreign tourists in USA.	
Preventive detentions.	Guardian Media Group (2011a)	UK	UK dissident citizens	
Complaints against governmental bad practices denouncers.	US News and World Reports (2013)	USA	USA journalists	
Public investment in centers for massive processing of espionage data.	Wired (2014)	USA	Internet users	
Unfulfillment of European regulations concerning citizen's rights.	Scheneier (2015)	Ireland	European Facebook users	
Unauthorized Police mass video surveillance.	Lippert and Newell (2016)	France	Football matches assistants	
		Spain	Pedestrians of conflictive suburbs	

Source: Own elaboration.

Table 3. Corporative ICT-based privacy management practices

Practice	Publication	Corporation(s); affected collective(s)
Individual privacy violation.	Electronic Frontier Foundation (2016a)	Acxiom; USA Internet users.
Delivery of users' data to governments without those ones' knowledge.	Wired (2011), Nash Holding (2013).	Amazon, Apple, AVM Software, Facebook, Google, Microsoft, Skype, Yahoo, Youtube, CNN, Fox News, MSNBC, Mastercard, Paypal Holdings, Visa, AOL; their respective users.
Reduction of available credit without any previous warning.	Credit Info (2008).	American Express; American Express users.
Publication of 'anonym' browsing profiles.	AOL (2006), The New York Times (2006).	AOL; AOL users
Privacy policy involving support to authorities in illegal activities prevention.	AT&T (2016).	AT&T; AT&T users.
Surveillance based on Internet activity.	Mashable (2012).	CNN; CNN customers.
Lobbying on USA government to achieve favoring legislation.	Electronic Frontier Foundation (2016a), Tribune Company (2011).	Facebook, Google; their respective users.
Surveillance of users' communication and delivery of the results of such surveillance to authorities.	Pell and Soghoian (2014).	
Participation in the global surveillance network.	Mashable (2012), Nash Holding (2013).	Amazon, Apple, AVM Software, Facebook, Google, Microsoft, Skype, Yahoo, Youtube, CNN, Fox News, MSNBC, Mastercard, Paypal Holdings, Visa, AOL; their respective users.
Massive surveillance of clients' activities in Internet.	Mashable (2012).	Fox News; Fox News customers.
Frequent changes of privacy norms.	Google (2016a, 2016b).	Google; Google users
Hide of the privacy policy's scope.	Internet Archive (1999).	
Lack of guarantees regarding fee services.	Vaidhyanathan (2011).	
Integration of each user information piece available in, or inferred from, its platform.	The New York Times (2012a).	
Attempt to appropriation of the information uploaded by users into its platform.	LinkedIn (2016b).	Facebook; Instagram users.
Violation of the journalist deontological code.	Guardian Media Group (2011b).	News Corporation; News Corporation clients.
Electronic surveillance.	Ramonet (2010)	Olivetti; Olivetti employees.
Access to its customers' Internet information accesses.	The New York Times (2012b).	Target; Target customers.
Sale of GPS data.	Daily Mail & General Trust (2011b).	Tom Tom; Tom Tom customers.
Lobby against regulations protecting infants' digital information privacy.	Tribune Company (2011).	Google, Twitter; their respective users.

Source: Own elaboration.

Highlights

- Mass surveillance is institutionalized in North America and Europe
- Social control and surveillance are carrying out by governments through ICTs
- Irregular personal information are carrying out by corporations through ICTs