Chapter 75
Privacy in the 21st Century:
From the "Dark Ages" to "Enlightenment"?

Panagiotis Kitsos
University of Macedonia, Greece

Aikaterini Yannoukakou
University of Macedonia, Greece

ABSTRACT

The events of 9/11 along with the bombarding in Madrid and London forced governments to resort to new structures of privacy safeguarding and electronic surveillance under the common denominator of terrorism and transnational crime fighting. Legislation as US PATRIOT Act and EU Data Retention Directive altered fundamentally the collection, processing and sharing methods of personal data, while it granted increased powers to police and law enforcement authorities concerning their jurisdiction in obtaining and processing personal information to an excessive degree. As an aftermath of the resulted opacity and the public outcry, a shift is recorded during the last years towards a more open governance by the implementation of open data and cloud computing practices in order to enhance transparency and accountability from the side of governments, restore the trust between the State and the citizens, and amplify the citizens' participation to the decision-making procedures. However, privacy and personal data protection are major issues in all occasions and, thus, must be safeguarded without sacrificing national security and public interest on one hand, but without crossing the thin line between protection and infringement on the other. Where this delicate balance stands, is the focal point of this paper trying to demonstrate that it is better to be cautious with open practices than hostage of clandestine practices.

INTRODUCTION

There is a unique paradox in modern society; that of citizens claiming for more privacy and protection of personal data on one hand, whereas governments pledge for increased surveillance measures adopting legislation, which stands on the edge of legitimacy as many advocate. Surveillance public cameras, x-ray devices looking under clothing, thermal motion detectors, wiretapping, devices like "Carnivore" or virus like "Magic Lantern" to record keystrokes (Solove, 2004), and many more are simple examples of how governments can tail and tag electronically their citizenry. The compari-

DOI: 10.4018/978-1-4666-8111-8.ch075

sons to "Big Brother" of Orwell's novel "1984" or to Foucault's Panopticon device are inevitable.

Especially after the 9/11 attacks, there has been a coordinated effort from governments worldwide to increase surveillance on the grounds of terrorism and organized crime, which led to a frenzy in adopting analogous legislation and regulation and employing technological solutions that ultimately outwit the basic constitutional rights of a citizen. Regardless if Solove (2004) has categorized surveillance as good (in Panopticon's case which functions preventative providing people with the choice not to engage in criminal activities) and bad (in Big Brother's case which suppresses the individuality and imposes authoritative governance), the fundamental question on where is the balance between the two remains.

In parallel, there has been an ascertained swift towards a more open, transparent and participatory governance during the last years as depicted to a number of initiatives (Open Government Movement, Open Knowledge Foundation, The Sunlight Foundation) and pieces of legislation (US Open Government Directive (2009), UK Open Data White Paper (2012), EU Open Data Strategy (2011)) and expressed with the use of open data in public administration that came as a respond to the increasing demand for more transparency and accountability on the workings of the governments and the opposition to the opacity practices employed the years followed 9/11.

The main objective of the paper is to examine whether privacy and openness coexist and the conditions necessary to achieve that. We determine privacy not only as individual's right to decide which of the information concerning it will be circulated, but as the obligation of the administrative State to safeguard this right both from the third parties and the government itself, especially via the implementation of surveillance laws. Even though this issue is under discussion for many decades, however we consider the 9/11 as the catalyst for altering the legislative scenery on privacy and access, not in a positive way in our opinion, as it assigned excessive power to government and law enforcement authorities, whereas at the same time limiting the exercise of the well-established right of access to information as defined by the Article 19 of Universal Declaration of Human Rights. For that reason, we commence our research with the US Patriot Act and expand it to EU Data Retention Directive, as they have proven to be two very controversial pieces of legislation, which have received severe criticism even from within. We do not oversee the impact of the previous surveillance and privacy legislation, but in our generation of growing the aftermath has been immense with most immediate results to our daily activities. So our research developed around the intension of demonstrating the changes that have been materialized globally privacy-wise after 9/11 and how governments worldwide hastened to adopt stricter surveillance policies, which in our opinion were unnecessary and clearly violated the right to privacy.

Moreover, we intend to demonstrate that the new tendency for open government is the only way to the future as it is being depicted to several initiatives adopted worldwide both by governments and non-governmental organizations. We support that privacy and openness are the different sides of the same coin, and actually do complement each other, whereas the more secure way to protect privacy is to re-built the trust between the State and the citizens and to adopt policies that embody privacy in the workings instead of preventative measures attempting to secure privacy as an aftermath. Also we consider privacy as a citizens' issue in the aspect of exercising their rights to review systematically the information held and processed for them by public agencies and to decided whether they wish to become informational object by designating which of the data should be publicized (Mitrou, 2001), whereas the non exercise of this right is synonymous to the unconditional consent towards the data holders to use the data as they deem appropriate.