

Protecting Privacy or Justifying Surveillance

A Critique of the Data Protection Authority Model

By Pablo Ouziel

Abstract: *The twenty-first century is rapidly evolving as a period in which powerful western democratic governments and others are advocating for an integrated global world of international standards and norms. In this world, multinational corporations have expanded their reach across continents to unprecedented dimensions. Technological developments, corporate lobbying, and governmental needs to control whole populations in order to offer services and defend from threats, have led to an increased use of surveillance instruments, mechanisms and tools. These increases, some claim are seriously infringing on our individual right to privacy, and are eroding the democratic ideals so many have worked hard to defend. Under this scenario, the battle for an individual's right to privacy is being fought on numerous fronts, in an array of Nation-States. Although there is no consolidated global movement defending the right to privacy, many advocates are beginning to acknowledge that a privacy battle lost in one part of the world quickly sets the precedent for a similar battle being lost in another place. Since Data Protection Authorities in most Western Nations are meant to be at the frontline of privacy protection, I feel strongly that academics can make key contributions to this ongoing debate by offering critiques of particular actions these authorities have taken.*

Introduction

On a recent research trip to Spain in which I was studying the development of the country's new electronic National Identity Card (DNIe), I had the opportunity of meeting former members of the Spanish Data Protection Agency who had worked on the agency's evaluation of the DNIe. During our conversations, I began to feel a grave sense of discomfort, as I acknowledged that their explanations of the identity card project paralleled those given to me by members of government, the police force, standards agencies, and international corporations involved in its development. Prior to my trip, I

had been studying the works of academics addressing privacy issues from an Anglo-Saxon perspective, through these readings, I had come to identify Data Protection Authorities as a valuable mechanism from which to defend our individual right to privacy. The disparity between the alleged role of Data Protection Authorities and the reality I witnessed on the ground in Spain, have propelled me to write this article. I hope the concerns I raise, will encourage debate on the control mechanisms needed to guarantee the effective working of Data Protection Authorities. Unless the public has ways of holding these agencies accountable for not ‘effectively’ defending their individual right to privacy, I fear that they will just become justifiers of surveillance and our privacy will be totally eroded.

This article does not intend to give specific solutions to the privacy debacle we are facing – that task is far too daunting –, rather, the article attempts to shed light on specific events, with the hope that it will encourage serious questioning of our genuine expectations for the role of Data Protection Authorities. This said, although the article will point to specific actions carried out or comments made by (or about) Spain’s Data Protection Agency, this piece can in no way shape or form be considered a case study of the agency.

Data Protection and Spain’s new National Identity Card (DNIE)

On the 2nd of March 1944 Generalissimo Francisco Franco Bahamonde approved an executive decree, which made it compulsory for Spanish citizens to have a national identity card. In 1951 the first cards were expedited. Since then, the card has witnessed

numerous changes to its design, the data collected, and the norms regarding its operability. Every change has been implemented by decree, making amendments to existing law; a new law has never been drafted.

On the 23 of December 2005, the royal decree 1553/2005 was approved, which regulated the expedition of the new National Identity Document and its certificates of electronic signature. In June of that same year, the *Comisión de Libertades Informaticas* CLI (Commission for Computer Freedoms) had asked to appear in front of the senate to address concerns regarding the launch of the new identity document. It was not until the 1st of December that the appearance took place in front of the *Comisión de la Sociedad de la Información y del Conocimiento del Senado* (Senate Commission for Knowledge and the Information Society). Due to this request by the CLI, the senate also asked for the appearance of the different ministries involved in the DNIe project, the police, and Spain's Data Protection Agency. During his appearance, the president of the CLI, Antoni Fariols, asked for a parliamentary debate in order to guarantee the correct implementation of the identity card. He also demanded that the government open a public discussion inviting all the affected groups, and expressed concern about the involvement of private interests, and the lack of involvement by the Data Protection Agency.

In a recent interview I conducted with Antoni Fariols, I learned there was much interest in a speedy approval of the identity card. As he elaborated, the time allocated to the senate commission for amendments to the project was cut from one month to ten days. He also pointed out that an evaluative study conducted by the commission was presented

in less than one month, when in fact it was expected to take four. According to Farriols, because the Spanish Data Protection Agency was part of a high commission with the vice presidency of the government, it rejected all criticism and quickly approved the project without demanding a parliamentary debate. The outcome of this has been over 10 million electronic identity cards already expedited. As stated by Juan Crespo¹ – chief inspector of Police and head of the Identity Card project – soon Spain will be the country in the world with the highest number of electronic identity cards in the hands of its citizenry. Furthermore, Crespo acknowledges that part of the reason the Spanish population has total acceptance of the document, is the seal of approval it received from the Spanish Data Protection Agency.

The Role of the Data Protection Authority

In 2006, the Surveillance Studies Network produced a report for the UK’s Information Commissioner’s Office (ICO), which stated that “where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance” (House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09). In a recent interview I conducted with Emilio del Val Puerto – currently at the Data Protection Agency of Madrid and previously in the Spanish Data Protection Agency dealing directly with the implementation of the DNIe –, he told me that the Spanish National Identity Card is an administrative control of the Spanish

¹ Juan Crespo shared this information with me during a recent interview I conducted.

population. For this reason, if we are to follow the 2006 definition made by the Surveillance Studies Network, we can safely say that the DNIe is a surveillance tool.

In *Surveillance Society*, David Lyon reminds us of the fact that “the vast bulk of responses to surveillance come under the rubric of protecting privacy” (Lyon 2001, 128). On a similar note, David Flaherty acknowledges that, “experience in all countries demonstrates that bureaucracies initially resist data protection, and that only legislative bodies can impose such controls upon them” (Flaherty 1989, 304). For this reason, Data Protection Authorities are meant to operate as ‘alarm systems’ for the protection of privacy, because at least this way, they can act as temporary barriers to the expansion of surveillance. From Flaherty’s perspective, the crucial role of the Data Protection Authority is to furnish leadership “in the federal public sector by serving as a catalyst for protecting personal privacy and by articulating privacy interests in every relevant situation” (Flaherty 1989, 305).

The European Community’s 1995 Directive sets standards for privacy protection for all its members and demands that they create an independent supervisory authority – role played by the Data Protection Agency in the case of Spain. Nevertheless, as James Rule highlights in *Privacy in Peril*, “the directive leaves open the same questions raised by other codes of ‘fair information practices’- notably, just how much of life should be subjected to mass surveillance” (Rule 2007, 32). In my view, it is the absence of this question, which separates the actions of the Data Protection Authorities from the interests of the citizenry. Surveillance practices can be perfectly legal, yet undesirable when

measured under ethical or moral criteria. “This may be particularly true where the legal rules are based on primary or secondary legislation that has not been sufficiently scrutinised by Parliament” (House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09). The Spanish identity card project seems to clearly reflect this reality. Although the whole process was kept within legal boundaries, and all technical issues were properly addressed, the lack of parliamentary or social debate concerning the implementation of the new technology seems undesirable. Considering the fact that the project has cost the Spanish tax payers over 400 million Euros (distributed amongst a select group of private corporations) and the card incorporates a new microchip with the citizen’s biometric data (also stored in a centralized database in the custody of the police), it seems to me, that an effective Data Protection Agency would have at least demanded a parliamentary debate and would have encouraged a social one.

In a statement that resonates with the Spanish reality, David Flaherty has genuinely acknowledged that data protection authorities risk simply becoming “agents for legitimating information-collection activities and new information technology” (Flaherty 1997, 175). Something, which is exposed by James Rule when he states that, “in many settings, regulation has apparently inoculated surveillance institutions against public indignation” (Rule 2007, 32). What he refers to as “disarming public objection” (Rule 2007, 35). Flaherty has also suggested that the role of data protection agencies is to raise consciousness at various levels of society (Flaherty 1997, 172). Unfortunately, this aspect seems absent from the handling of the DNIe project by the Spanish agency. When I

explicitly asked members of the agency involved in the project, whether they felt their role was to inform the citizenry about the involvement of private corporations, their answer was, no. They then proceed to explain that their role is to deal with the technical and practical issues. In their minds, the role of informing the public about whether a particular company with ethically dubious dealings is involved in any data protection related project is the task of investigative journalists and NGOs.

Aware of the fact that the present reality is not ideal, looking into the future, things do not look any brighter, and certainly in the case of Spain, the Data Protection Agency doesn't seem poised to defend our privacy interests. Rule has warned of the fact that "once national databases of entire populations exist, state agencies of all sorts find uses for them that may never have been announced, or even anticipated in advance" (Rule 2007, 162). In the case of Spain, the one body which should protect the citizens from such evolutions – the Data Protection Agency –, aware of the fact that the legal tools are in place for this to happen, was comfortable putting its seal of approval on the DNIE without the blink of an eye. Expressing my concern about the data inserted in the card's microchip and the centralized database – during my time with the Data Protection Agency – I asked whether the government could demand in the future more information from the public. The answer was clear: "As long as the intention is the same as the one for which the DNIE was created, which is to identify Spanish citizens, then the government could very well through decree add new requirements for data collection without having a parliamentary debate. This could include introducing demands such as iris scans" (Emilio del Val Puerto).

With today's technological advancements, for either well-meaning or malevolent regimes there are no natural limits to the incorporation of personal information in systems of mass surveillance. For this reason, I find disturbing the acknowledgment made by Emilio del Val Puerto regarding the database of Spain's identity card: "It is possible that a dictatorial government would have it much easier in Spain than in many other countries to do a profiling of the society." One cannot minimize the importance of having an effective Data Protection Agency; as David Lyon points out, the gains achieved in the legal realm of data protection and privacy law are numerous, yet as he stipulates, they have severe limitations. Perhaps the most important limitation as Bennett and Raab have emphasized, is the fact that Data Protection Authorities "are themselves part of the system" (Bennett and Raab 2003, 253). This obstructs their ability to ask the right question, namely, "what purposes, what interests warrant creating and maintaining surveillance systems?" (Rule 2007, 24).

Concluding remarks

It seems apparent that in regards to its dealings with the DNIe, the Spanish Data Protection Agency approved the project purely based on legal and technical aspects, forgetting – or choosing to ignore – the importance of a long and sustained parliamentary debate, and an in-depth analysis of the social forces and power structures involved in the development of such a privacy invading project. It is incredibly worrisome, that aware of the inherent surveillance creep and acknowledging that such a policy instrument facilitates profiling, the agency should offer its seal of approval to the project. As Rule states, "privacy advocates have hurt their cause by acquiescing to, or even promoting,

notions that privacy is somehow compatible with relentless efficiency maximization in government and private institutions” (Rule 2007, 192). A PowerPoint presentation used by the Spanish Ministry of the Interior promoting the DNIE as a tool with “more security in a privacy compatible way” (Ministry of the Interior 2006, 29), offers a vivid example of this last point. Moving forward it is clear that things need to change.

In order to seriously confront the threats to privacy arising from ever-increasing surveillance assemblages, individuals concerned with these issues must stop trying to maintain an ever-weakening illusion of privacy and shift to the offensive by demanding accountability from those whose power is enhanced by the new initiatives (Stalder 2002, 123). Unless we do so, I fear that Flaherty might be right when he warns that a full-fledged surveillance state is “almost impossible to prevent in the long term, whatever the prodigious efforts of data protectors and their allies” (Flaherty 1997, 170).

Privacy advocates around the world must question the Spanish Data Protection Agency’s handling of the country’s National Identity Card, and acknowledge that the project represents a lost privacy battle. The fact that it is a lost battle for all concerned advocates is demonstrated by Stork, a project, which has received 10 million Euros in funding from the European Commission to consolidate and integrate the new identity cards of various European countries. Rapidly, electronic identity cards are mushrooming across the globe, in some countries privacy advocates are able to temporarily resist, in others, Data Protection Authorities are quickly delivering the coup de grâce by stamping their seal approval. After years of subversive battles, the time is approaching for a full-frontal war.

Those concerned with their privacy rights must determine whose side the Data Protection Authorities are on. Currently their name seems in contradiction with their actions, at least in the Spanish scenario.

Bibliography

Bennett, C.J. and Raab, C.D. (2003) *The governance of privacy: policy instruments in global perspective*, Surrey: Ashgate Publishing

Flaherty, D. (1997) 'Controlling surveillance: can privacy protection be made effective?' in *Technology and privacy: the new landscape*, edited by Philip E. Agre and Marc Rotenberg, Cambridge MA, MIT Press.

Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, London: University of North Carolina Press.

House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09, available online at:
<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm>

Lyon, D. (2001) *Surveillance Society: Monitoring everyday life*, Philadelphia: Open University Press.

Ministerio de Interior (2006) *DNI electrónico*, available online:
<http://www.terena.org/activities/eurocamp/april06/slides/day2/victoriano-giralt.pdf>.

Rule, J.B. (2007) *Privacy in Peril*, Oxford: Oxford University Press.

Stalder, F. (2002) 'Privacy is not the antidote to surveillance' in *Surveillance and Society* 1 (1): 120-124.