

# **Balancing Identification and Privacy in the Age of Routine Surveillance**

*By Pablo Ouziel*

***Abstract:** The incremental use of surveillance mechanisms has been a part of our 'evolution' for centuries, however, over the last few decades, aided by technological developments and the ingenuity of man, a new kind of 'routine surveillance' has arisen. In this innovative form, surveillance systems demand that individuals identify themselves in order to access required services. The outcome of this has been an increase in the volume and size of the 'digital dossiers' held by organizations – created with the identifiable personal information of individuals. This in turn, has led to an increase in the possibilities of identity theft; a growing insecurity concerning the secondary use of personal information; and a growing risk of destabilizing the balance of social and institutional power in our societies. For this reason, routine surveillance poses a threat to our democracies, and therefore, I hope that privacy scholars dedicate time to studying the consequences of the routine use of identifiers, on the privacy rights of individuals and society. This article aims to contribute to such analysis.*

## **Routine Surveillance and the need to identify Privacy as a Collective Value**

In her 1980 work, *Privacy and the Limits of Law*, Ruth Gavison points to the fact that perfect privacy is impossible to achieve in any society. Furthermore, she reminds us of the fact that total loss of privacy is equally impossible to achieve. Although few would dispute these words, in the early days of the twenty first century, it can safely be argued that privacy is rapidly being lost, as increasingly, individuals become the subject of attention of other individuals and organizations. This as Gavison herself points out, is “true whether the attention is conscious and purposeful, or inadvertent” (Gavison 1980, 432). For this reason, if we take privacy to be an essential element of a democratic society – which “fosters and encourages the moral autonomy of the citizen” (Gavison

1980, 455) –, we must reflect seriously on the infringements upon privacy currently taking place in our societies.

Advances in surveillance technologies and the constant developments experienced in the field of database design and storage capacity, together with an inherent interest within our societies to know more about others; have made it almost impossible to protect the same levels of privacy enjoyed by democratic societies only a few decades ago. Under this new paradigm, privacy is rapidly becoming a “*collective value*”, in that technology, market forces and governmental demands, are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy (Regan 1985, 213).

Adding to this concept of collective privacy, Priscilla Regan emphasizes, that since “the nature of the relationships that generate records and information is changing, it is hard to define these relationships as truly voluntary” (Regan 1985, 229).

In the modern democratic state, for virtually everything most of us need to do – obtain work, pay taxes, go to the doctor, open a bank account, and drive a car –, we are asked to release personal data. Due to technological progress, this data can be easily recorded and reconstructed in minute detail. A situation that leads Spiros Simitis to conclude, that surveillance has lost its exceptional character and become routine practice (Simitis 1987, 710). As part of this routine surveillance, individuals are increasingly confronted with demands to identify themselves in order to access required services. It is this demand for identifiable personal information, which Simitis claims, is “increasingly used to enforce standards of behavior” (Simitis 1987, 710).

Considering the fact that the accuracy and efficiency of these routine surveillance systems is constantly improving as their costs are lowered, while data sharing abilities have improved greatly; privacy activists have to acknowledge the fact, that for democratic societies the risk of these developments are high. The increased possibility for the “labelling of individuals, manipulative tendencies, magnification of errors, and strengthening of social control, threatens the very fabric of democracy” (Simitis 1987, 746). It is this sense of an increasingly worrisome threat, which compels me to analyse the relationship between identification, surveillance and privacy. By undergoing this work, I seek to understand contemporary developments taking place at the core of our democratic societies. Achieving this aim requires an understanding of identification, identifiers, the dependence of most routine surveillance practices on personal identification, and the effects of identifiers on our universal right to privacy. In the next section of this article, I offer an overview of these issues, and I finalize with some concluding remarks and questions, which I consider relevant for further research into this topic.

### **Identification, Surveillance and Privacy**

Identification is the association of data with particular individuals. Within designated contexts, identifiers enable relying parties to distinguish between the individuals they interact with (Brands 2006, 208). Identifiers are always connected to a physical individual or organization. As a component of many routine forms of surveillance, identifiers facilitate “the detection and monitoring of a person and enable surveillance data to be categorized according to the individuals to which it pertains” (Solove 2006,

512). According to Daniel Solove, since identification reveals, distorts, and intrudes, even if no information is revealed publicly, it is still capable of creating harm. This does not mean that identification has no positive elements. For example, the verification of a person's identity in many instances can be a step towards the reduction of fraud and the enhancement of accountability.

Today, there are many types of identifiers which are requested by organizations in order to fulfil specific transactions, some of these include birth names, email addresses, telephone numbers, fingerprints, DNA samples, social security numbers, credit cards, passports, drivers licences, employee badges, IP addresses, and RFID tag identifiers.

From a privacy perspective, these identifiers are not the actual reason for concern. The problem, as numerous scholars and activists have highlighted, regards the fact, that these identifiers empower information collectors by linking data to particular individuals: "Because it connects people to data, identification attaches informational baggage to people" (Solove 2006, 511), which can prevent self-development as individuals seek to escape from their past.

In his widely cited *Privacy and Freedom*, Alan Westin speaks of various states of privacy, one of which, he describes as anonymity. This he claims, "occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance" (Westin 1967,31). On a related note, Solove points to identification as the inhibitor of anonymity, and reflects on the fact that anonymity protects people from bias based on identity, and enables citizens to execute their

democratic rights of voting, speaking and associating freely – “by protecting them from the danger of reprisal” (Solove 2006, 513). Both these writers have frequently been lauded as architects of the privacy debate. At the same time, there is a broad consensus in our societies in regards to our understanding of privacy, as the ability of individuals to minimize what personal information relying parties can learn beyond what individuals choose to explicitly disclose. Nevertheless, as a society we are constantly adopting identifiers without much questioning, as the most effective way of conducting our daily transactions. As we do this, we provide an ever-growing number of identifiers to an ever-growing number of organizations, in an ever-growing number of situations. This gives relying parties increased capabilities for linking and tracing. From Solove’s perspective, this poses ‘architectural’ privacy problems: “They involve less the overt insult or reputational harm to a person and more creation of the risk that a person might be harmed in the future” (Solove 2006, 487).

Supporting the concerns addressed by Solove, Stefan Brands claims that although identifiers offer protection to relying parties vis-à-vis the individual whose personal data is requested, they offer no privacy and security for the individual. In his article, *Secure User Identification Without Privacy Erosion*, Brands elaborates on this topic by outlining a few points, which support his claim. Namely, that identifiers provide the basis from which all actions of individuals can be traced and linked; that relying parties can make discriminatory decisions based on identity, and can also arbitrarily blacklist individuals; and finally, that others can steal or forge identifiers to impersonate target individuals (Brands 2006, 214). Contributing to this last concern, Solove emphasises that identity

theft is made increasingly easy because “we all have ‘digital dossiers’ – extensive repositories of personal information about us – that are maintained by various companies and institutions” (Solove 2006, 515). He also raises awareness to the fact, that the potential for secondary use of personal data creates a sense of “powerlessness and vulnerability”, and reminds his readers of the broader overarching risk, that the growth of digital dossiers can inadvertently “upset the balance of social or institutional power in undesirable ways” (Solove 2006, 487).

### **Concluding remarks**

Colin Bennett has reminded us of the fact, that the job of the academic is to interpret the world and not to change it (Bennett 2008, 78). Acknowledging his advice, this article has not attempted to change anything, but has tried to interpret different conclusions reached by respected contributors to the privacy debate. Surveillance is with us, and although some say it is here to stay, I refuse to adopt such a complacent position. Surveillance as I see it evolving, bothers me. The more I study its meaning and consequences, the more concerns it raises. Nevertheless, I refrain from behaving as an activist in opposition to it, in order to obtain the necessary academic rigor, required for shedding light on its evolution. *Function and volume creep*, is a concept I recently heard being used by a renowned Privacy Scholar, in order to define the evolution of surveillance. My own observations of surveillance developments in Western democratic societies, draws me to this statement.

As a collective, the population of most Western societies has adopted identification as the legitimate and appropriate way to interact in the majority of our everyday activities. Information which in the more rudimentary societies of our past, was considered private and intimate – and only shared with a few –, is today in the era of big government and large multinational corporations, shared with impersonal and distant organizations. This task is greatly facilitated by the use of highly sophisticated databases with data mining capabilities – dependent on identifiers, in order to match specific data to a particular individual. Aware of the benefits of providing certain data, and clear about the consequences of refusing to do so; on many occasions citizens seem more than willing to provide identifiers, as they are requested by different organizations. A clearly illustrative, yet extreme example of this last point is that of the need to show a personal identifier (such as drivers licence, or passport) to board an airplane. Despite the fact that travellers have the option not to show their identifier if they are willing to remain on the ground; it is safe to assume, that most western citizens faced with the need to travel on an airplane, would rather show their identifier and have it read through digital devices – which the majority of citizens do not understand –, than to have to cancel their flight. Assuming that an individual agreed to offer his or her identifier and boarded the airplane, would this constitute a voluntary sharing of personal information? If we take into consideration the fact that in today's modern states, many of the activities which could be labelled as 'normal', require some form of identifier which links to our physical identity; it seems to me, that the term 'voluntary' has become redundant in many instances of routine surveillance.

This creeping loss of privacy demands that we ask ourselves serious questions. Should we pay more attention to the dangers posed by the existing ‘digital dossiers’ of our personal identifiable information? Does the demand for identifiers, which constitutes a cornerstone of most routine surveillance, represent in anyway a breach of our privacy? How could privacy scholars contribute to this debate? Finally, another important question is as follows: If as academics our role is to interpret the world, not to change it. Who should work on the changes, if we ever interpret that something is fundamentally wrong? Answering this last question might generate the opportunity for a 360° reversal in the growth in scope, volume, and sophistication of surveillance practices most modern societies have quietly interiorized.

From Ruth Gavison, we have learned that “there are important limits on our capacity to change positive morality, and thus to affect social pressures to conform”. This situation can lead to an absence of privacy, which can destroy “the lives of individuals condemned by norms with only questionable benefit to society” (Gavison 1980, 453). From Daniel Solove, we received the warning on excessive social control through routine surveillance mechanisms. A perspective, which ‘threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspiration to it’ (Solove 2006, 494).

From my analysis of the issue at hand, I am able to interpret the following clear points; that our collective value of privacy is being drastically reduced; that as a collective group of citizens we have adopted personal identifiers as routine tools for everyday

transactions; and that ‘digital dossiers’ pose serious threats to the balance of social and institutional power in our cherished democracies. This process of identifier collection has rapidly accelerated in just a few decades and there are no visible signs indicating that things are about to change.

## **Bibliography**

Bennett, C.J. (2008) *The Privacy Advocates*, Cambridge MA: The MIT Press.

Brands, S. (2006) ‘Secure User Identification Without Privacy Erosion’ in *University of Ottawa Law & Technology Journal*, Vol. 3, No. 1, 2006

Gavison, R. (1980) ‘Privacy and the Limits of Law’ in *The Yale Law Journal*, Volume 89, Number 3, January 1980.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values and Public Policy*, Chapel Hill: University of North Carolina Press.

Simitis, S. (1987) ‘Reviewing Privacy in the Information Society’ in *University of Pennsylvania Law Review*, Vol. 153, No.3: 707-46.

Solove, D. J. (2006) ‘A Taxonomy of Privacy’ in *University of Pennsylvania Law Review*, Vol. 154, No.3: 477.

Westin, A. F. (1967) *Privacy and Freedom*, New York: Atheneum.