Tranvik, Tommy

Security and Privacy
Year of birth: 1968
Nationality: Norwegian
Present professional position: Researcher, Research Center for Computers and Law (NRCCL), Faculty of law, U. of Oslo
Main interest of research:
Two latest publications:
- Tommy Tranvik (red): Digital teknologi og organisasjonsendring : studier av offentlig og frivillig sektor, Paperback | 223 sider | Fagbokforl. | 1. utg. | 2008 | Bokmål | ISBN: 9788245006636
- Tommy Tranvik; Per Selle: Digital teknologi i sivilsamfunnet, Paperback | Unipub forl. | 1. utg. | 2008 | Bokmål | ISBN: 9788274773530

Privacy and Security: Being Watched or Not Being Watched?

Introduction

The relationship between security and privacy is not easily conceptualised. Partly because what some people regard as necessary security measures may be regarded by others as unnecessary restrictions on our privacy. And partly because there is little agreement about what privacy actually is – it is a concept without a “hard core” – which means that it is not entirely clear what diminished or increased privacy means.

Privacy is therefore defined in very many ways, for instance, in terms of intimacy, personal integrity, the right to be let alone, the right to be secure in your communication with others or the right to exercise some measure of control over information about yourself. It is particularly the right to exercise some form of control over personal information that is emphasised in today’s Data Protection Legislation. This means that the protection of personal information is one way of achieving privacy.

Security is an even more elusive term, but it seems to be intimately linked to surveillance – surveillance is one of the tools we use to achieve greater security.[1] The argument that is often made is that the closer we are watched, the better – more civilised, more responsible and less deviant – we behave. In this way, surveillance leads to more security and less privacy: dangerous or so-called anti-social behaviour can be detected and corrected by increased surveillance and, consequently, by diminishing our privacy. What we can say, then, is that privacy has something to do with groups or an individual’s right not to be watched, while security has something to do with the social benefits (less crime, for instance, or reduced welfare fraud) that can be harvested from being watched.

And this is how the security-versus-privacy debate is usually framed. The recent discussions concerning the European Union’s Data Retention Directive is but one example. Here, the question is whether the collection of information about all sorts of private electronic communication will help fight crime, terrorism, drug trafficking, etc., or if it will undercut our privacy and undermine our data protection rights?

[1] Surveillance is the monitoring of behaviour – the behaviour of people, of machines and of various types of social or technical processes – to make sure that the behaviour in question confirm to expected norms (and are corrected if it does not).

What I will do in this short paper is, first, to give a short and rather biased account of the security-versus-privacy-argument – the idea that the closer we are watched, the better we behave – as it has been developed and refined within the social sciences. Second, I will argue that being watched or not being watched is perhaps not the big security-and-privacy question. It is perhaps just as important to ask "how are we being watched and by whom"? What are the rules of the game and do we need new rules? But, first, who has decided that security and privacy cannot be friends – that they do not like each other very much?

The Security-versus-Privacy Debate

In recent history, the most influential people to have promoted this idea seems to have been the early students of modern organisations – people like Max Weber, Fredrick Taylor and Henri Foyal. They argued that on the factory floor or inside large-scale public bureaucracies people (employees) were managed in a new way: they were closely watched so that they would produce more and better goods and services much faster than before. So, large-scale industrial workshops and other organisations started monitoring and controlling their employees in order to make sure that productivity-goals set by management were fulfilled (today, this philosophy is at the heart of public sector reforms that are collectively referred to as New Public Management). But, according to these theorists, this form of workplace surveillance turned industrial and public bureaucracies into iron-cages, where the privacy and autonomy of employees was traded away for more management oversight, increased productivity and efficiency (in contemporary society, the workplace surveillance debate is focussing on issues like the employer's right to read employees e-mail or to get access to information about Internet use).

In the late 1960s, another group of social scientists started making a similar argument: we can call them the Big Brother theorists (for instance, Alan Westin, Arthur Miller and James Rule). The Big Brother theorists were especially concerned about the rise of the computer and of large databanks that big businesses and big governments employed to manage their affairs. The argument that was made back then – and that is still made today – is that when fast computers are linked to various types of electronic watching-systems, the society as such is managed like the workshops of the industrial age: the watching that earlier took place on the factory floor has now moved outside the factory gates. Consequently, private lives are exposed to public surveillance so that the needs and wishes of "the little man" can be managed, controlled and (hopefully) satisfied by an army of faceless bureaucrats. Even as this argument was being made, the first data protection laws were introduced, and the first Privacy Commissioners or Data Inspectorates saw the light of day.

If we fast-forward another 20 years – to the late 1980s or early 1990s – the risk society approach (which was made famous by Ulrich Beck and others) takes the security-versus-privacy-argument one step further. It is now claimed that security risks have gone global – for instance, your credit card number can be hijacked over the Internet by organised gangs in South East Asia or your website can be hacked by the Russian mafia. And in a world of global risks, security is king. So, when security risks are global and largely unknown (it is hard to know about risks that may originate on the other side of the world, for instance, in the mountains of Afghanistan), the privacy of ordinary people – the so-called data subjects – are traded away for the perceived benefits of increased surveillance. The point, according to this argument, is that security is more important than privacy because the basic challenge facing the risk society is the protection of local or national assets in a global, dangerous, fast-changing and competitive environment.

The Security-versus-Privacy Debate Revisited

This very short account of the security-and-privacy-argument means that as we move from the factory floor via the Big Brother society towards the risk society, the basic argument stays the same – more security means less privacy (the closer we are watched, the better we behave) – but the details, or the way this argument is presented and defended, change. It also shows that in the minds of some social scientists the future of privacy is not very bright: despite some positive developments (for instance, the much-talked-about but rather elusive privacy-enhancing technologies and new things like identity management), a silver lining is hard to spot.

But this may not be all we need to know about security and privacy. As I have already indicated, it is not at all certain that more surveillance and security can only be achieved at the expense of privacy. A more important question may be how to secure some measure of privacy even as we are closely watched. I will give one example to demonstrate what I am talking about here: information security and local government in Norway.

Local government in Norway collect and use all sorts of personal data in order to provide health care, social services, education, and so on. I have studied how 18 municipalities are handling all this data, especially regarding how security needs and privacy interests are balanced against each other. The first thing to note is that although some social groups may be a more closely watched today than before (like, for instance, suspected welfare cheats) those who provide the actual services are concerned about the privacy of their clients. Even if municipal employees collect and handle lots of personal data, they do not see this as a form of surveillance, but as the basis for the best possible service or care (but, of course, it may be experienced as surveillance by those at the receiving end). Privacy, or data protection, it seems, is something that many welfare professions worry about. This may indicate that even big, computerized bureaucracies – those who do a lot of watching – may not be insensitive the privacy interests of individuals (at least not to the extent that some of the social scientists referred to above would like us to believe).

The second thing to note is that the security-versus-privacy debate looks very different on the municipal level than it does in many social science textbooks. And the type of security I am talking about here is information security, particularly confidentiality: how to prevent improper disclosure of personal and, especially, sensitive data.[2] On the municipal level, information security is not – at least not openly – prioritised at the expense of data protection. Rather, a concern for data protection (or privacy) seems to lead to a concern for information security since both concepts highlights the issue of confidentiality: keeping personal information secret is one of the primary aims of both data protection and information security work. This overlap between data protection and information security can in part be explained by how the relationship between these two concepts is defined by the new Data Protection Act of 2000. This piece of legislation stipulates that information security is a significant part of the data protection regime that those who are doing the watching – municipalities, for instance – are required to implement. But it is nevertheless an open question whether or nor information security actually promotes the data protection interests of ordinary people. Take, for instance, the issue of access control. Access control means that municipal employees should only be able to access personal data on a need-to-know-basis (the data they need in

[2] Confidentiality is only one aspect of the information security concept. The other two are integrity (prevent unauthorised users from modifying personal information) and availability (prevent unauthorised users from withholding or deleting personal information).

order to do their jobs). But, according to the Norwegian Data Inspectorate, there is great confusion locally about who should get access to what type of information, and this problem is usually solved by giving everyone access to nearly everything (for instance, all or much of the information contained in electronic journals). Obviously, this may not provide for good data protection or information security.

Also, this lack of data protection and information security may create all sorts of interesting problems. For instance, because of inadequate access control, medical personnel (doctors, nurses, etc.) may take it upon themselves to protect the confidentiality of their patients' data by not entering medical information into the electronic journal. So, if you are a nurse on night-watch that is responsible for a patient connected to a machine that is supposed to go blip, but now all of a sudden goes blop, you know that the patient is in trouble. But you do not know what that the trouble is because the patient's doctor (who is on vacation) has decided not to write up all the relevant information in order to protect the privacy of his patient. This exemplifies the complex nature of the relationship between security and privacy: too little information security may provoke informal and privacy-enhancing actions (not entering medical information into the journal) that can have serious and unintended repercussions.

In addition, some of the provisions of the Data Protection Act may cause information security and data protection challenges: Many municipalities, it seems, have difficulties understanding what the Act requires them to do (and what not to do), especially when it comes to the information security. The information security regulations are based on straight-forward risk management principles (and are therefore similar to those we find in, for instance, the health and safety legislation), but risk management, and what it entails, is poorly understood. The result is that the responsibility for information security is often handed over to the IT-department on the assumption that this is technical stuff that we – the top management – do not need to take seriously. But if information security is removed from the top management's agenda, it may be doubtful if the actual security work will be as supportive of privacy and data protection as was probably intended when the Act was passed.

Conclusion

So, to wrap up this short presentation: Lawyers and data authorities have recognized that information security and privacy are not inherently contradictory concepts, and, of course, so does privacy or data protection laws. Even so, much of the public debate is framed as a tug-of-war between security and privacy: more security, less privacy (the closer we are watched, the better we behave). This debate seems to be informed by the views promoted by the early "factory-floor-theorists", the Big Brother people and the risk society people. But in modern societies it seems unlikely that surveillance-and-security-policies are a sort of fashion – something that will soon go away so that we can enjoy the privacy we once had. Instead of debating how to beat back surveillance, we should perhaps be discussing how the watching should be done and who should be doing it.

Local government in Norway is one arena where this debate is ongoing. Here, it is not assumed that privacy and security (i.e. information security) cannot be friends. Instead of viewing these two concepts as enemies, they are (for the most part) regarded as supportive of each other. How supportive of each other they actually are, is an empirical question. The answer to this question will depend on, for instance, how well the Data Protection Act is understood and how local employees interpret the privacy and security needs of the users of municipal services.