amsterdamlawforum
VU University Amsterdam

KEEPING OUR SURVEILLANCE SOCIETY NON-TOTALITARIAN

Bart Jacobs[*]

Introduction

In 2006 the United Kingdom information commissioner Richard Thomas warned that we are "sleepwalking into a surveillance society". He referred to the increased recording and monitoring of people's behaviour, for instance via security cameras, various smart cards (for identification, loyalty, access, transport), data retention for (mobile) phone and email communication, automatic number plate recognition (ANPR), radio frequency identification (RFID), biometric verification and identification, and so forth. The introduction of these relatively new techniques and measures has been a gradual process, proceeding in small steps, each with its own rationality, but whose cumulative effect has brought us into a surveillance society, as is also argued by OHarrow and Murakami Wood.[1] This article will sketch the development and characteristics of this surveillance society, especially in relation to computer security, privacy and autonomy. The phrase 'surveillance society' will be used in a morally neutral manner, intended to capture a characteristic of modern, technologically advanced societies.

Surveillance societies have mechanisms for monitoring, influencing and controlling people in their private lives. These mechanisms may be used for commercial, political or security reasons. In case the authorities actively use these mechanisms to monitor, influence and control people in their private lives on a large scale, the term 'totalitarian society' will be used, in line with the terminology of Hannah Arendt.[2] Hence totalitarianism does not refer to brutal, physical suppression – this is what Arendt associates with tyranny – but to the interference with personal affairs. There is no sharp boundary between (passive) monitoring and (active) influencing/controlling, since knowing that you are being monitored in your private life has, in general, implicit influence on your behaviour.[3] However, for the purposes of this paper, deliberately exerting explicit influence and control in private lives is considered part of the idea of a totalitarian society, not of a surveillance society. One may argue that a transformation of a surveillance society into a totalitarian society is primarily a matter of politics, not of technology. It is

[*] *M.Math., M.Phil., Sc.D. (Nijmegen), www.cs.ru.nl/BJacobs. The author would like to thank colleagues Marcel Becker, Jaap-Henk Hoepman, James McKinna and Wouter Teepe for their helpful critical comments..*

[1] R. OHarrow Jr., *No Place to Hide*, New York: Free Press 2005; D. Murakami Wood, editor, *A Report on the Surveillance Society*, UK Information Commissioner's Office 2006. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (accessed on 24 August 2009).

[2] H. Arendt, *The Origins of Totalitarianism*, New York: Schocken Books 1951.

[3] Metaphorically, monitoring of private life is like measurement in (non-classical) quantum physics: it changes the state of the system being observed.

not so easy to say that once the tools for easily exerting influence are in place, the threshold for using them becomes lower. Hence it becomes an issue itself whether or not we should introduce tools that can be abused easily in the first place, and if so, under what (technological) restrictions and safeguards.

This paper is to a large extent descriptive in nature. But it does make a moral stand: it discusses regulations and techniques to reduce (or mitigate) monitoring of private lives, and to resist influence and control. The mechanisms of a surveillance society are extremely useful in totalitarian societies. The issue of potential abuse is thus a serious one that will have to be faced explicitly. Preventing our surveillance societies from becoming totalitarian is one of the major challenges of our time. The emergence of populist movements in Europe, with their limited care for fundamental civil rights, may be seen as making this matter more urgent. However, these political developments are left outside the scope of this article. Rather, the focus will be on regulation and use of technology itself, via five concrete guidelines that may be summarised as: 'select before you collect', 'decentralised storage of personal information', 'revocable privacy', 'attributes instead of identities', and 'reactive, non-proactive policing'.[4]

I. Computer Security, Privacy and Architecture

Computers have a deep influence on our society, via our dependence on electronics in general, in particular PCs, mobile phone and digital databases. We have become dependent on easy communication and storage of digital information, and on efficient mechanisms for searching and recognising patterns in large databases. Also, we have realised that in many situations such information needs to be properly protected, for instance in relation to national security, commercial or personal interests. The (sub)discipline of computer security focuses on the regulation of access to digital assets. Privacy can be seen as an intrinsic part of computer security, as far as it concerns techniques for the protection of personal information. Of course, privacy is a much broader topic.[5]

Information could be protected by putting it in a safe and dumping it to the bottom of the ocean, however this makes access a bit difficult. Regulation of access means that the 'good guys' can get access to the (protected) assets, but the 'bad guys' cannot. In computer security encryption (or encipherment) of data makes data unreadable: it corresponds to the storage of information in a safe box. Encryption cryptographic keys are parameters, which are (functionally) comparable to physical keys for safe boxes. These cryptographic keys are very large numbers. They are far too large to remember and are typically stored in the protected memory of chip cards. They are used to encipher or decipher data. Modern, computerised encryption of data is so complex that it can be regarded as practically irreversible, unless you possess the appropriate cryptographic key.

[4] See Section VI.

[5] See also Section III.

An important aspect of computer security is key distribution: making sure that the good guys possess the appropriate cryptographic keys, and the bad guys don't. As a result, it is important to know who is accessing information. Typically one distinguishes the following three aspects:

- **identification**: telling who you are, for instance via your family name, login name, bank account number, passport number, social security number, *et cetera.*;
- **authentication**: proving who you are, for instance via a (physical) key, a password, a PIN, an official document, or a biometric (like a finger print, or iris scan);
- **authorisation**: deciding who is allowed to do what.

Traditionally, computer professionals have been the architects of the digital world. Increasingly, they are also architects of the social world. Information is power: the one who has most access to information also has most power to exercise influence (over others). The information architecture of a computer system determines the flow of information and thus who sees what, and which information is protected. Computer security issues and concerns about privacy and societal division of power meet at this point. Mitchell Kapor is one of the founders and the first chairman of the Electronic Freedom Foundation (EFF), an international non-profit organisation that aims to defend civil rights in the digital age. He has coined the phrase 'architecture is politics'.[6]

Here is a concrete example. Many countries are considering replacing their flat road taxes with a form of road pricing based on actual road usage. Cars are then equipped with special devices containing GPS functionality, to determine a car's location, and GSM functionality, for communication. An obvious 'centralised' architecture requires that these devices send location information to a central database, say once every minute. Based on this information bills can be calculated and sent to car owners. An alternative 'decentralised' architecture keeps this (privacy sensitive) location information in the car and requires that the devices themselves calculate the bill, based on a tariff map. In the first architecture the (road pricing) authorities can monitor the whereabouts of all individual cars in detail, whereas in the second architecture they cannot. This clearly involves more than just a technical choice, as is also argued by De Jonge and Jacobs.[7] Computer architectures thus have social and moral significance: they are not value-free.

[6] See also L. Lessig, *The Future of Ideas*, New York: Vintage 2001.

[7] W. de Jonge & B. Jacobs, 'Privacy-friendly electronic traffic pricing via commits', in P. Degano, J. Guttman, and F. Martinelli, editors, *Formal Aspects in Security and Trust*, number 5491 in Lect. Notes Comp. Sci., pp. 143 - 161. Berlin: Springer, 2009; and B. Jacobs, 'Architecture is politics: Security and privacy issues in transport and beyond', 2009: http://www.cs.ru.nl/˜bart/PAPERS/cpdp09-jacobs.pdf (accessed on 24 August 2009).

II. Individual Autonomy

The modern idea of the individual, for instance since Kant, is that people are simply autonomous and free, within reasonable bounds, to take their own decisions. Modern democratic societies are built on this view. This section illustrates that the situation is not so simple and that in practice states have an essential role in shaping and safeguarding this individual autonomy – even increasingly so with the growing importance of technology. In brief, this section revolves around the following two points: (1) individual autonomy is fragile and vulnerable, and (2) democratic societies have various mechanisms to protect this autonomy. These points will be illustrated by three examples.

II.1 Voting

The voting systems in democracies are regulated by precise laws. Interestingly, developments towards electronic forms of voting, via computers in poll stations or via the internet, have led to a renewed investigation of the underlying principles, including vote freedom, vote secrecy, and verifiability of voting.[8] These laws and principles protect people and almost 'force' them to make an autonomous choice. For instance, poll stations are protected environments where political messages and advertisements are not allowed. There are separate voting booths, in which only one person at a time can enter to cast a vote on one's own without any influence from outside. Also, people do not get any form of proof of how they voted, in order to prevent coercion or buying of votes. Apparently democratic societies think that such protection of individual autonomy is needed.[9]

II.2 Advertising

In marketing it is not very effective to send bulk advertisements to every possible customer. Experience shows that it has little effect to advertise expensive cars in poor neighbourhoods. Targeting works much better, whereby specific advertisements are sent only to specific groups or individuals. The combination of surveillance of individuals and marketing leads to 'behavioural targeting'. Information about your behaviour – which programs you watch, which websites you visit, where you live and travel, what and where you buy, how much you earn, save and spend – is important input to compile a personal profile of you. Such a profile can be used to send you very specific, focused advertisements, which can be worded in a style that is assumed to appeal to you. These advertisements may even use price differentiation, so that the price that is presented to you depends on your financial situation (or behaviour). Some people get irritated, others see it as a

[8] See for example the recommendation adopted by the Council of Europe, 'Legal, operational and technical standards for e-voting', September 2004. Recommendation Rec (2004)11 adopted by the Committee of Ministers of the Council of Europe, with explanatory memorandum: https://wcd.coe.int/ViewDoc.jsp?id=778189 (accessed on 24 August 2009).

[9] In postal voting or voting via the internet many of these protection mechanisms are not present and so the risk of what is called 'family fraud' is much higher. This is seen as a serious disadvantage of such forms of remote voting.

helpful service, and others are simply not able to resist well-targeted seductions. Already a certain percentage of the population cannot cope with aggressive advertisements, such as for commercial loans, leading to political debate: for example, in 2006 Dutch parliament discussed banning aggressive loan advertisements, but in the end it did not happen. It may be expected that with the growth in behavioural targeting additional regulation is needed to protect individual autonomy.

II.3 Interrogation

Without going into specifics of particular countries, several miscarriages of justice have been attributed to the way police interrogations are conducted. Apparently, people can be influenced to confess to crimes that they did not commit. This shows the fragility of individual autonomy. In response to such miscarriages of justice additional protection mechanisms have been called for, ranging from videotaping of police interrogations to (earlier) presence of defence lawyers.

III. Privacy

Privacy is a broad topic that is traditionally studied in legal and ethical literature.[10] It is under pressure in our surveillance society, especially when it concerns the increased focus on public security after the 9/11 attacks. Privacy is construed as an obstacle to public security, notably in phrases like: "if you have nothing to hide, you have nothing to fear".[11] However, while privacy is essential for personal security it is a soft value that is relatively hard to defend. The way privacy is understood often only involves the issue as to whether or not others learn about or monitor your behaviour (*cf.* Big Brother). But when passive monitoring turns into active influencing and controlling, autonomy and freedom of interference is also at stake (*cf.* Kafka). The two notions of privacy and autonomy are closely related.

In our lives we are all involved in different roles: for example at work, in church, in the pub, in hospital, at home, or in a social (online) network. Associated with each role is a special context or sphere in which certain information may be relevant, in one way or another, depending on the context. Privacy may be best understood, in a fairly concrete way, as individual control over the exchange of information between one's own different roles in society.

Some people choose to have fairly little separation between these roles, and make for instance much of their personal life public in a social network or in online blogs. In this case they are still in control. Learning how to exercise such control over personal information is becoming an integral part of

[10] See for example Schoeman, who provided an overview: F. Schoeman, editor, *Philosophical Dimensions of Privacy. An Anthology*, Cambridge Univ. Press, 1984.

[11] D.J. Solove, "'I've got nothing to hide" and other misunderstandings of privacy', *San Diego Law Review*, 44, 2007. GWU Law School Public Law Research Paper No. 289: http://ssrn.com/abstract=998565 (accessed on 24 August 2009).

growing up, as can be seen with youngsters who experience that putting too much information online can harm them or make them vulnerable.

Suppose you have a Pay-TV subscription. The company involved will typically keep track of which films you watch, if only to compile a bill.[12] The information of what you watch in your private home environment is thus stored somewhere else outside your control. The database containing who-viewed-what-where-and-when may become public, as a result of hacking, or negligence. Maybe some acquaintance works for the TV company and can look up in the database what you watch. This reduced informational control, if you are aware of it, probably feels like a loss of privacy. Is it also a loss of autonomy? That depends on you. Do you still switch on an embarrassing or controversial film (say with Nazi or communist or fundamentalist propaganda) if you know that this fact will be added to your personal customer profile and may become known to others, beyond your control? Pay-TV companies are usually not very explicit about this monitoring and profiling of their clients. At most they mention it in the small print in terms of "collecting information to improve our level of service to individual customers".

Via such surveillance mechanisms, information about what we do in one specific context is stored somewhere else, outside this context and outside our own control. This may apply to an online shop, or to your local library or video rental or a supermarket that keeps track of what you buy via membership or loyalty cards. Banks and telecommunication companies also store lots of sensitive personal information. In presence of data retention laws the information is kept longer than commercially needed.

Alternative decentralised architectures with local, in-context, storage of sensitive information do exist but have been hardly explored or used in practice. They reduce the power of the service providers (and authorities) and require more involvement and effort of individuals. In the end, it is of course a matter of whether we care enough to handle our data ourselves, and if so, if we manage to convince or (democratically) force organisations to switch to such decentralised architectures.

IV. Data Mining

[12] It is not really necessary that the company keeps track of what you watch. It can also be organised that you keep track of this data yourself, in a fraud resistant manner. For instance, the company may send you a statement, each time you view a movie, digitally signed by (devices of) both you and the company. The statement may say that you viewed this movie at such-and-such time, and keep only a hash of this signed statement itself, together with a cumulative bill. In case of a dispute about the bill, you will have to produce the pre-images to these hashes, which can be checked by the company. There are however very few incentives for a Pay-TV company to introduce such a privacy-friendly, decentralised architecture.

Computerised handling and monitoring of our daily transactions yields enormous databases containing our digital footprints. Powerful, query-based search techniques make it possible to extract pieces of information that are relevant for a specific purpose — as with Google. A different, more holistic form of analysis of such vast amounts of data is called 'data mining'. It involves the large scale, automated statistical analysis of data. Roughly speaking, data mining can be used in two different ways, namely to test an already existing hypothesis, or to discover new relationships between data elements. It is important to note that data mining only yields statistical patterns, and no causal relationships.

Here is a simple example. Suppose that a (grocery) shop keeper wants to know which products are often sold together, so that she can put them closer together on the shelves in her shop, with the idea that customers who buy one product are possibly tempted to also buy the other one. Data mining can help in such a situation: first, one compiles a substantial collection of lists of products bought by individual customers (whose identities do not matter here). Then one searches these lists, one by one, while counting the occurrences of all possible pairs of products. This may yield obvious pairs of products with frequent occurrences, like taco chips and chilli sauce, less obvious ones like bean soup and toilet paper, or strange combinations like dog food and French blue cheese. Unexpected patterns may emerge, without any clear causal connection or explanation. Still they may be useful, commercially.

Via data mining new, high-level information can be extracted. For instance, supermarkets can find out, through their loyalty cards, when their female customers have their periods. When one analyses individual shopping data spanning many years one expects that a (statistical) pattern emerges, since female customers are more likely to buy feminine hygiene products during certain periods in a month. This information could be used for timely, personal advertisement. However, it would probably shock many customers if such personal information was exploited so openly, precisely because it forms a privacy breach: information from one (intimate) sphere is used in quite another one, without consent. Supermarkets apparently respect the privacy of their (female) customers by not extracting and using this kind of information. But the information is in principle available out of context. Similarly, mobile phone companies know which of their (male) customers frequent prostitute areas. It is also unlikely that this information will be exploited commercially. Many more examples, ranging from political micro-targeting to personality grouping in dating services are described by Baker (without much reflection).[13]

The information obtained via data mining is often not 100% reliable. This is not so problematic in a commercial context when it results in a mistargeted advertisement. But when a mortgage is denied to you purely based on a data

[13] S. Baker, *The Numerati,* Boston, New York: Houghton Mifflin Comp. 2008.

mining analysis you may feel unfairly disadvantaged and demand to know precisely what is going on. That is why the European directive 95/46/EC[14] forbids that such decisions are made purely automatically and requires human intervention. However, in practice this is problematic.[15]

Data mining can thus uncover hidden patterns that can be used to compose profiles of individuals. These patterns/profiles may be used *a posteriori* (reactively) or *a priori* (proactively), in an anticipatory manner. An example of the first use is credit card fraud detection: if your profile says 'European traveller, small expenses' and your card is suddenly used for a big transaction in Bangkok, alarms are raised and the transaction may be blocked.[16] In this case the 'act' (of buying something in Bangkok) takes place – or is at least initiated – and triggers a reaction. Profiles are used proactively, if the 'act' is prevented from happening in the first place. Examples include when you were denied a loan because your profile indicated that you are a high risk candidate, or when you are not allowed to board a plane, because your profile says 'potential terrorist' (no local but many international phone calls, recent visit to Pakistan, you ordered an *halal* meal and an aisle seat, and so forth.).

An important aspect of (European style) privacy laws is that people have the right to inspect what information on them is stored, and to require correction or even deletion under certain circumstances. These laws were written at a time when data mining was still in its infancy. It is not clear whether the right to inspection only applies to the stored personal data itself, or also to the derived personal profiles, or even to the selection mechanisms that are used in data mining. After all, in many situations it is quite reasonable that you have a right to know the rules that are used in data mining and in blocking or stimulating certain behaviour on your part. Such knowledge is quite relevant for fair and possibly effective forms of appeal.[17]

IV.1 Data Mining for Public Security

Police and intelligence services are beginning to use data mining as a tool in public/national security. This is controversial, partly because of association with 'precrime', as in the film Minority Report (2002), in which a special police unit prevents criminal acts before they happen by pre-emptive arrests based on intentions (knowledge of which is obtained via 'precogs'). This is not far from reality because there is for example a new development in policing in the Netherlands to take selected people briefly into custody before major events, like high-risk football matches or visits of heads of states, based on profiling.

[14] See especially articles 12 and 15 (Directive 95/46/EC).

[15] M. Hildebrandt, Profiling and the rule of law, *Identity in Information Society (IDIS)*, 1, 2008. http://ssrn.com/abstract=1332076 (accessed on 24 August 2009).

[16] In practice these fraud mechanisms have so many false negatives today that the credit card itself is no longer a reliable means to pay.

[17] See for further discussion: A. Vedder, KDD: 'The challenge to individualism', *Ethics and Inf. Technol.*, 1(4): pp. 275 – 281, 1999; and Hildebrandt (2008), *supra* note 15.

Data mining and profiling involves many statistical uncertainties, which are only aggravated when the databases are polluted and contain errors. This is often the case, possibly resulting in a propagation of errors. But in public security both false positives (the good guy is seen as bad) and false negatives (the bad guy is not detected) are unacceptable. Once you are flagged as 'bad' the presumption of innocence (you are innocent unless proven guilty) may no longer be distinct. The burden of proof may be put on you, to show you are not guilty, instead of on the police authorities, to build up a case that you are guilty.

After the 9/11 attacks data mining was seen as one of the promising tools to detect potential terrorists early on, before they would strike. After some years the enthusiasm has faded away. A recent critical report by the U.S. National Academies involving many experts and stakeholders has advised against the technique: there is too much data (needle in the haystack problem), which is often 'soft' and unreliable, there are too few clear signs of terrorist activities, and there are too many ways for terrorists to generate obfuscating and misleading signals. Data mining is not the way to find an extremely small, well-hidden group in an extremely large population.[18]

V. Surveillance Society Characteristics

The brief anatomy of a surveillance society in this paper has focused on the following three characteristics.

1. Being free increasingly requires being shameless. In principle, the extensive monitoring that characterises a surveillance society does not force you to behave in a certain way. You are, in principle, still free to make your own choices, as long as you do not care about the fact that the resulting behaviour is being monitored and leads to information storage out of context. If you don't care that other people know that you watch (say) adult films, via your Pay-TV subscription or via IP-addresses stored at online servers, you quite happily and freely switch them on. But if you do feel ashamed, the (knowledge of the) fact that you are being monitored may inhibit you.

Interestingly, certain religions describe God as all-seeing, often with possible disciplinary consequences, in the hereafter or already in this life. The intimate relationship between panopticism and discipline was studied by French philosopher Michel Foucault in his writings on prisons.[19] The panopticon style prisons designed by Jeremy Bentham may serve as model for society as a whole, where citizens are becoming transparent and are monitored

[18] Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, *Protecting Individual Privacy in the Struggle against Terrorists*, Washington: The National Academies Press, 2008.

[19] Foucault wrote about the whole prison system as a way of keeping control of unwanted elements in society, see M. Foucault. *Surveiller et punir: Naissance de la prison*. Gallimard, Paris, 1975. Translated as: *Discipline and Punish: The Birth of the Prison.*

constantly, but are never sure whether their digital traces are actually inspected or not.

2. There is no clear separation between passive monitoring on the one hand and active influencing and controlling on the other. Data mining techniques make it possible to extract hidden patterns from information obtained from monitoring. These patterns are easily used, both reactively and proactively, to steer behaviour in a certain direction. Often the patterns are extracted exactly for this reason. This disciplinary effect may take the form of self-censorship: when you know that certain behaviour patterns will trigger a reaction, and thus hassle ("step out of the line, please, and come with us"), you may decide to behave in a more conformist manner. The greater the uncertainty about what precisely is stored in your profile and triggers a reaction, the greater the fear and tendency towards conformism. Conformism is however not what has made western societies excel (industrially or scientifically, for instance).

3. In case political power in a surveillance society falls into the wrong hands of (internal or external) parties with malicious intentions, they will be happy to find many surveillance tools standing ready for totalitarian use. Historically the most prominent example is the effective use that Nazis made of citizen administrations in continental Europe to single out Jews. Current tools offer far more options for controlling the population, as can be seen in several countries today.

VI. Controlling Surveillance

Are we sleepwalking into a totalitarian society? Is there an unstoppable and inevitable process? The main concern is of course to make sure that power does not come into the wrong hands, namely of those who want to deliberately use it to maliciously control and suppress the population. But maybe a totalitarian society emerges in just the same way that the surveillance society arose: in small steps, each of which was understandable from a narrow perspective and not completely devoid of rationality. Each further optimisation of the surveillance society allows us to detect and catch more bad guys, to prevent crimes from happening in the first place by extensive profiling of the entire population and pre-emptive arrests or other interventions, and to reduce the overall risk. Maybe a new totalitarian society provides a safe and comfortable environment for the majority, in which we will be shameless enough to feel sufficiently free, in which profiling is never explicit and individual behaviour is steered primarily via personalised seduction, and in which the authorities behave like omniscient parents and will not openly abuse their power, at least not against the conformist majority. Is this realistic, and do we want such a society? With each further optimisation of the surveillance society we accept more monitoring and control, and implicitly express faith in all future governments.

The incident-driven focus on functionality of surveillance mechanisms makes it difficult to see the bigger picture and to develop a vision of what is going on and of where we want to go. One aim of this paper is to try and snap out of the sleepwalking, by presenting some building blocks that could form part of a more conscious and controlled (and dignified) form of surveillance society. Some of such building blocks are presented below, as possible alternatives.

VI.1 Select before you Collect

Traditionally in a state of law one first has to become a 'suspect' before certain surveillance restrictions can be lifted in lawful investigations, including phone tapping, searches, information seizure. Hence the traditional order is: first select (a suspect), then collect (information). Increasingly this order is reversed and information is collected first (about everyone), and subjects to be investigated are selected later. The clearest example[20] is the European directive 2006/24/EC, on telecommunications data retention which prescribes that all 'traffic data', capturing who communicates with whom and when and where (but not the content) of all 450M European citizens have to be stored for a fixed period of time.[21] This is the surveillance society at work. Bowden wrote: "Traffic data constitutes a near complete map of private life: whom everyone talks to (by e-mail and phone), where everyone goes (mobile phone location co-ordinates), and what everyone reads online (websites browsed). At present, the geographic coordinates of a mobile phone can be tracked to within a few hundred meters whilst the phone is switched on. The new 3G (third generation) phones will pinpoint location to a few meters".[22] Apart from privacy concerns, such a 'collect before you select' approach is problematic because it treats everyone as a possible suspect. The data retention directive is highly controversial, and is contested in constitutional courts, for instance in Germany.

Sticking to the 'select before you collect' principle is an important aspect of limiting surveillance and limiting the possible options for abuse.[23] Data may be collected and stored about selected people, if there is a proper reason, but blanket collection of data without any reason (yet) is to be avoided.

One objection to such a limitation of blanket collection is that the selection of suspects becomes more difficult. But in practice, this does not seem to be a real problem. It seems that in almost all the publicly known terrorist attacks

[20] But there are more examples: some countries, like the Netherlands, are planning to store finger prints of all citizens with a passport (criminal or not) in a central database that is accessible for law enforcement.

[21] At least half a year and at most 2 years; member states can choose the exact retention period themselves; many of them choose at least one year. An evaluation of the directive is foreseen in 2010.

[22] C. Bowden, 'Closed circuit television for inside your head: Blanket traffic data retention and the emergency anti-terrorism legislation', *Computer and Telecomm*, Law Review, 2002. Available from Duke Law & Techn. Review, http://www.law.duke.edu/journals/dltr/articles/2002dltr0005.html (accessed on 24 August 2009).

[23] B. Jacobs, 'Select before you collect', *Ars Aequi*, pp. 1006 – 1009, December 2005 (in Dutch): http://www.cs.ru.nl/B.Jacobs/PAPERS/jacobs-arsaequi-dec05.pdf (accessed on 24 August 2009).

(or attempts) the terrorists involved were known to, and often even under surveillance of, the police and intelligence communities, before investigative powers as in the data retention directive existed. The signs may not have been interpreted correctly, but that is another matter. Also, as shown in the report 'Protecting Individual Privacy in the Struggle against Terrorists'[24] mining in large scale databases is not the proper way to find terrorists. Selection involves human (police) work, based on skills and experience. It involves more human intelligence (*humint*) than 'signals intelligence' (also known as *sigint*).

VI.2 Decentralise Data Storage

Centralised databases full of privacy sensitive information may be attractive for the database owners (or the authorities), but are not necessarily attractive for the subjects involved. Concerns exist about the 'information is power' issue and about the large number of data loss incidents,[25] making incidents structural. New models and architectures are needed to handle such sensitive information, together with the political will and societal pressure to introduce them. In Section III privacy has been described in terms of control over exchange of ones own personal information between different spheres in ones life. The ability to keep personal information within the original context is thus important for privacy. This requires (new) architectures for decentralised storage of data, as in the road pricing example at the end of Section I. Another recent, controversial example is the introduction of electronic electricity/gas/water meters in private homes, which regularly transmit, every 15 minutes for instance, the usage levels to a central server at the utility company. This involves a move in the opposite direction, from local, decentralised storage in traditional meters, to centralised storage via electronic meters.

Decentralised storage can be done using smart cards, like in the German health card *Gesundheidskarte* that stores an abstract of the medical record of the card owner. Other personal devices, like phones or PDAs, can also be used. But the physical location of the information is not so important – it may be anywhere on a grid networks long as it is encrypted and the required cryptographic keys are controlled by the data subject. By the use of appropriate digital signatures it can be ensured that the data is authentic, so that local tampering is not possible (or at least is detectable). These decentralised architectures may be flexible, so that people also have the option to store their personal data in the traditional centralised way, but the important point is that they should be able to choose this themselves – in line with the concept of privacy as informational self-determinacy.

VI.3 Revocable Privacy

[24] National Research Council (2008), *supra* note 18.

[25] See for instance http://datalossdb.org/ for overviews (accessed on 24 August 2009).

The idea behind car number plates – before automatic number plate recognition – is that you can drive around reasonably anonymously, but if you violate a law, bystanders or police officers can write down your number plate and look up who you are. This may be seen as an example of revocable privacy. There are modern, digital versions of this idea. The most famous one is digital cash as proposed in 'Untraceable electronic cash'[26]: digital coins are big numbers with the identity of the coin-owner embedded arithmetically. The problem with such coins – like with any digital datum – is that they can be copied arbitrarily many times. But the system is designed in a clever way so that a certain check takes place when you spend a coin, in such a way that (only) upon double spending of a coin, the embedded identity pops up, via a clever calculation with these numbers/coins.

The essence of revocable privacy is to design systems in such a way that no personal information is collected centrally, unless a user violates a pre-established policy. Only in that case, personal information (and violation details) are revealed to the authorities. Privacy protection is thus not an add-on but is built deeply into the architecture of the system, and does not rely on legal or procedural safeguards that can be changed or circumvented relatively easily. Revocable privacy is in line with the 'select before you collect' adagium from Subsection VI.1 and may be a way to (partly) reconcile the justifiable interests of law enforcement and privacy protection.

VI.4 Attributes instead of identities

Section I described the three notions of identification, authentication and authorisation. Many forms of authorisation do not require identification (and authentication), but only 'attributes', such as being over 18, having a valid ticket, being a citizen of a particular country, and so forth. Often such attributes are related to an identity, but such a connection is not strictly necessary. If you need to prove that you are over 18, for instance in a liquor shop, by showing an identity card, you give away much more information than strictly necessary, certainly if this card can be read electronically – and all your personal data can be joined with your stored purchase history. This additional information, including possibly your social security number, can be abused in various way, leading to what is called identity fraud. In the digital age identity-poor solutions[27] are needed, involving for instance electronic attributes that are digitally signed by appropriate authorities.

Unfortunately, the move is still in the other direction. For instance with the introduction of smart card-based ticketing in public transport, travelling has suddenly become identity-based (see also Jacobs).[28] These smart cards have a fixed identity, that shows up every time you use it. In many cases it is

[26] D. Chaum, A. Fiat & M. Naor. 'Untraceable electronic cash', in S. Goldwasser, editor, *CRYPTO 1988*, number 403 in Lect. Notes Comp. Sci., pp. 319–327. Berlin : Springer 1988.

[27] I.e. to be understood literally: involving as little identity information as needed.

[28] Jacobs (2009), *supra* note 7.

connected to a personal identity – or can easily be linked to an identity, for instance via payment logs.

VI.5 Reactive Policing only

Section IV has described the controversial character of data mining, in particular in relation to public security. After the Second World War most European countries did not want their intelligence services to be a secret policy (like the Gestapo of the Nazis). As a result, the intelligence community is organised differently from the police, without the power to arrest, but with more extensive information gathering powers, focused on forces that threaten the constitutional order. Hence it is natural that they make cautious use of data mining to uncover hidden patterns (while applying the highest information security standards to the sensitive data in their custody). For the police services this is less self-evident: in essence they are a reactive force, that takes action when the law is violated. There is pressure to make police work more proactive. This is uncontroversial when it comes to advising on safety precautions in homes, but active use of pattern-based data mining and developing personal profiles of all citizens is a different matter. Given the low threshold of errors and abuse in data mining, the combination with the operational powers of the police is not a fortunate one, since it involves extensive monitoring (and control) of private lives and may precipitate the move towards a totalitarian society. In a surveillance society there is an abundance of data that police officers can use reactively (and selectively, see Subsection VI.1.), in their investigations.

This subsection thus concludes with a simple but far reaching proposal: intelligence services should be allowed to use pattern-based data mining, for their restricted task, but police forces should not. Of course, this data mining should be used with a proper understanding of its pitfalls and limitations.[29]

Conclusion

The mechanisms for monitoring and controlling people are becoming so powerful that we need to 'stop and think' in order to slow-down the incident-driven focus on functionality and to develop a robust vision, if we wish to continue to protect individual autonomy, not only against aggressive commercial parties but also against over-active states that believe in blanket, non-selective monitoring and pre-emptive intervention. A broad vision, involving among other things a demarcation between surveillance societies and totalitarian societies, is not developed here. However building blocks for such a vision are sketched, with emphasis on selectivity, decentralised, in-context storage of privacy sensitive data, via architectures guaranteeing revocable privacy and attribute-based authorisation, and limiting the use of data mining and pro-active policing for public security. The 'positive' use of technology in order to protect privacy and autonomy is essential for this approach. It requires that we stop sleepwalking, become more aware of the

[29] See National Research Council (2008), *supra* note 18.

values involved in the design of technologies, and make some conscious and transparent choices.