Chapter 25

PRIVACY AND CIVIL LIBERTIES

D. Chadwick, M. Olivier, P. Samarati, E. Sharpston and B. Thuraisingham

Abstract This paper describes the proceedings of the panel on privacy and civil liberties. It presents the panelists' positions and considers the issue of privacy from the tecnological and legislative perspectives.

Keywords: Privacy, security, anonymity, accountability, civil liberties

1. Introduction by Pierangela Samarati

In today's global information society, an increasing degree of awareness with respect to privacy is inevitable. Privacy issues have been the subject of public debates and discussions and many controversial proposals for the use of information have been debated openly. In the United States as well as in many European countries, privacy laws and regulations are being demanded, proposed and enforced, some still under study and the subject of debates. Privacy is a complex topic. First, privacy – a right we all agree that everybody should indeed enjoy – may conflict with accountability, and then can open the door to abuses by malicious party. There are different views on how the trade-offs between security and privacy should be solved. Second, privacy is an interdisciplinary problem that requires the combined application of technology, law and public policy, and organizational and individual policies and practices.

On the basis of these two simple observations, the panelists were asked to provide their views on privacy in today's electronic society. Some questions were provided to start the discussion:

- What is privacy? (complete anonymity, unlinkability, ...)
- Privacy from whom? (everybody, your peers, your government, commercial companies selling data, ...)

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35697-6_26

E. Gudes et al. (eds.), *Research Directions in Data and Applications Security*

- Privacy vs. Security: Is there an acceptable trade-off? (protecting privacy of bad guys is dangerous ...)

- Privacy is not only technical: what contribution can computer scientists give?

The remainder of this chapter provides the panelists contribution to the discussion.

2. David Chadwick's Position

Firstly let us try to differentiate between pseudonyms, aliases, nicknames, anonymity, privacy and confidentiality. Anonymity ensures that others cannot determine your true identity. An anonymous person effectively does not have an identity. A pseudonym on the other hand is an alternative (fictitious or assumed) identity for a person. Aliases are identical to pseudonyms, but the two are used with different connotations in different contexts. An author may write books under a pseudonym, but their true identity may be widely known, whilst on the Internet someone may use a pseudonym because they don't want their true identity to be easily known. A person may have an alias email address to allow others to easily send email to them, but the police often state that a criminal is know by an alias name, which implies some unlawful purpose. Pseudonyms and aliases will usually not prevent the true identity of a person from being determined, although it may be difficult and may require law enforcement to enable it. Anonymity on the other hand should ensure that the true identity of a person is never found out, nor is capable of being found out.

A nickname is also an alternative name for a person, and is often chosen as a friendlier variant of the person's formal name. Nicknames are not chosen so that the person's identity can be hidden. On the contrary, they are meant to identify the person and are often chosen when several people share the same name, in order to uniquely disambiguate between them. Therefore nicknames won't be discussed further in this section.

Privacy (noun) is one's right to seclusion, secrecy and concealment. When applied to an object, it is the right that requires that others do not access it. The object can be a person, a life, or a document. We typically say that we want data privacy meaning that unauthorised users are not allowed to access the data. Confidential is an adjective that we attach to data to indicate that it is private. In data communications, encryption is the mechanism that we use to ensure that data remains confidential during transfer.

If a party in a transaction is truly anonymous this ensures that the other parties in the transaction are unable to determine his/her identity. Anonymity is relatively easy to achieve in real life every day transactions. For example, making a cash purchase at a market stall in a distant town is a relatively

anonymous transaction. The only records of the transaction are your fingerprints on the money (which can be avoided by using gloves), and the memories of the stallholder and nearby people (which can be obscured by wearing make-up and wigs etc.). Since anonymous transactions provide no identity and have a non-existent or inconclusive audit trail, the anonymous transacting party cannot usually be identified. Anonymity therefore enables or at least encourages criminality, since the chances of being identified and caught, when undertaking a fraudulent transaction, are slim. The converse is also true. Transactions in which all parties are reliably identified and authenticated to each other tend to discourage criminal activities, since the chances of being caught, when undertaking a fraudulent transaction, are high. Consequently, this section makes the proposition that *anonymity on the Internet is a bad thing, since it encourages criminality, and therefore should not be actively encouraged or supported.* However, true anonymity on the Internet is difficult to achieve. Many anonymous actions on the Internet, whilst being anonymous at the time of the transaction, leave significant audit trials behind that allow the identities of the anonymous parties to be uncovered. For example, many of the devastating viruses such as Melissa have left sufficient audit trials to allow their authors to be identified. Further, several papers that have described anonymous transactions on the Internet, are really describing pseudonymous transactions rather than anonymous ones, since the true identity of the "anonymous" party can be determined by contacting the trusted third party that knows how to map the presented "anonymous" identity into the true identity. A pseudonym is an assumed name or identity for a person. By its very nature, a pseudonym identifies a person. The true identity can usually be revealed via one or more direct mappings. In some cases it is relatively easy to determine the true identity of the pseudonymous person, in other cases it is not, and may require a court order or other instrument to reveal the true identity. Never the less, pseudonyms are fundamentally different to anonymous identities. The former have a direct link to the person, the latter have no link. Therefore pseudonyms do not encourage criminality to anything like the same extent as anonymity, since the pseudonymous person knows that the pseudonym can with greater or less effort be traced back to them. This section makes the second proposition that *where privacy is required, the use of pseudonyms on the Internet is a good thing and should be supported.*

This section also asserts that *data privacy on the Internet is a good thing, and that the owner of the data should be the person responsible for determining who is authorised to access it.* There is one caveat to this, namely: *that law enforcement should always be capable of being granted access to private data, irrespective of the wishes of the data owner, providing that they have good reason for this as determined by an independent judiciary.* There are a number of important points in the above. Data privacy is a good thing, since

confidential data in the wrong hands can do untold damage, usually to the data owner. Therefore if the data owner has sole responsible for determining who has access to his private data, then any damage that he suffers as a consequence of this can only be due (directly or indirectly) to him giving access to the data. It cannot be due to some other third party data custodian giving access to the data without the right to do so. Unfortunately most private data on the Internet today is not held by the data owner but by some third party, and the data owner is not able to specify who should have access it. For this reason the EC data protection directive is a good thing, since it endeavours to give the power back to the data owner.

Turning now to the above caveat, in some cases confidential data, for example, the names and addresses of co-conspirators who helped a suspect in a recent bank robbery should not remain private, since it is in the public good that this data be known to law enforcement. To take a slightly more complex example, if an accountant knows that his client has shredded some vital documents detailing a fraud that the client has committed, and the accountant has a copy of this data, then law enforcement should be able to obtain access to this data regardless of the wishes of the client or the accountant. Of course this assumes that we have a benevolent government and that the judiciary is independent and will only give law enforcement the right to access private data when they have sufficient reason to. But what happens when a government is not so benevolent, but rather is there to serve the purposes of a dictator? Or what if the judiciary is not independent and is perverted into serving the wishes of a non-democratic government? In these cases, anonymity and data privacy are essential for the well being of all citizens, and law enforcement and government agencies should not have the ability to determine the contents of private data or the identity of the owner. Otherwise citizens with views contrary to that of the prevailing government can be charged with sedition, subversion or other serious crime when they are expressing views counter to the government's, or documenting human rights abuses etc. The citizens now need to be protected as much, if not more, from their government than from criminals.

So ultimately we have a Gordian Knot, since it is in the interests of the citizens of a benevolent government that anonymity on the Internet should be discouraged, and data privacy should have the caveat of legal recourse to access the data. However, it is in the interests of the citizens of a malevolent government that anonymity on the Internet should be strongly encouraged and data privacy without any ability to access it should be supported. Unfortunately, one man's benevolent government is another man's malevolent one, and vice versa, and the Internet spans all shades of government in all countries. So ultimately what should be the solution for the Internet? Try to untie that one.

3. Martin Olivier's Position

The position I will defend here is that (1) technical solutions should be sought to enhance individual privacy[1] since social controls are insufficient on their own to guarantee privacy; and (2) if one errs with individual privacy, it is better to ensure too much privacy rather than too little privacy since privacy, once lost, cannot effectively be regained.[2]

The argument is structured as follows: the privacy problem is outlined and it is argued that privacy is a human right. Next it is argued that national and class differences regarding privacy are less important in IT. Finally, it is argued that societal protection on its own is insufficient. Many of my views expressed have been shaped by my history as a South African and I therefore deliberately try to use South African examples here when they are applicable. For the discussion here, I will define the privacy problem as ensuring security of personal information. Given that security hinges on confidentiality (or secrecy), integrity and availability [7, pp. 4-6], it follows that the privacy problem asks how best to ensure and balance these aspects for personal information.[3]

The notion of civil liberties or human rights is entrenched in most modern democracies and privacy is widely seen as one of these rights. Rights can usually only be limited by laws that apply to all citizens equally. The panel discussion reported on here took place less than a year after the 11 September 2001 incidents in the United States and this naturally posed the question: given acts of terrorism,[4] is it justifiable to require citizens (to an equal degree) to give up some right to privacy to prevent future similar occurrences?

John Rawls's *A Theory of Justice* is often used to consider questions of justness in such cases. His first principle of justice of institutions states that "each person is to have an equal right to the most extensive total system of

[1]Although the theme of the panel was *Privacy and Civil Liberties*, the panel discussion focussed almost exclusively on privacy. I will therefore limit most of my remarks here to privacy, except where a remark about civil liberties is needed to address privacy issues.

[2]From my position it follows that technical solutions that appear to be too strong should not be dismissed merely because of their potential to be misused. However, it does not imply that privacy is an absolute right.

[3]As formulated, the privacy problem is clearly a facet of the broader security problem and solutions to computer security problems are therefore of interest when the privacy problem is considered. The privacy problem, however, differs in at least two significant respects from the security problem: (1) whereas the security problem usually has to protect data owned by a single (or a few) owners (the organization), the privacy problem often concerns the protection of data owned by many private individuals; and (2) whereas the data to be protected by security solutions are typically stored on systems owned by the data owner(s), private data, once disclosed, is usually stored on a system not owned by the individual(s) concerned. Lack of space precludes a detailed discussion of the precise differences in solutions to the two problems; however, see the panel discussion of a previous conference for some examples [12].

[4]It should also be remembered that one person's terrorist is often another's freedom fighter. The 'old' South Africa expected citizens to sacrifice some civil liberties precisely to fight "terrorists or communists" [5, p. 626]; however Nelson Mandela [5, p. 336] emphasises that their acts during the liberation struggle were sabotage and not terrorism. Sometimes what is terrorism, is defined by who happens to be the most powerful; at other times it depends on who happens to be "on the [right] side of history" [5, p. 626].

equal basic liberties compatible with a similar system of liberty for all" [4, p. 163]. Since (presumably) citizens will be expected to sacrifice the same degree of privacy, it may seem that Rawls's theory supports such a sacrifice.

Since acceptable mechanisms are in place to collect information about an individual about whom reasons for suspicion of unlawful activities have been demonstrated, it means that a new *sacrifice of privacy* goes beyond the existing mechanisms.[5] A sacrifice of privacy for security therefore implies that the intention is that privacy should be sacrificed by all, to identify suspicious activities of individuals for whom suspicion has not been demonstrated. Clearly, those people whose opinions, languages, ethnic origins, or other personal attributes differ most from the dominant view, will attract the most attention.[6] Again Rawls [4, p. 163] provides us with some insight: "a less extensive liberty must strengthen the total system of liberty shared by all," and, more importantly for the current discussion, "a less than equal liberty must be acceptable to those with the lesser liberty." Clearly then, if a decrease in the level of personal privacy afforded inhabitants of a country will place the spotlight more intensely on members of specific groups – primarily because they are members of those groups – the decrease in privacy level should be acceptable to those groups.[7]

In summary, one should be critical of attempts to limit civil liberties. "Violation of privacy has a normalizing surveillance function, channeling members of society into standard behavior and turning deviates into perverts" [6, p. 205].

Next the nature of privacy needs to be considered. Margalit [6] gives a number of examples to explain that what is considered private is culturally dependent and also depends on social class. These dependencies make it impossible to clearly state what information about an individual should be considered pri-

[5]Technologies that restrict such lawful 'infringement' of privacy have been discussed elsewhere. Consider Philip Zimmerman's arguments in favour of encryption (PGP) and arguments in favour of and against the US Government's proposed use of key escrow in combination with the use of the Clipper chip.

[6]To illustrate the point that, when groups are targeted, individuals become vulnerable, consider the well-known events following the Japanese attack on Pearl Harbor. In February 1942 advisers wrote to President Roosevelt "In time of national peril, any reasonable doubt must be resolved in favor of action to preserve the national safety, not for the purpose of punishing those whose liberty may be temporarily affected by such action, but for the purpose of protecting the freedom of the nation, which may be long impaired, if not permanently lost, by nonaction" [13]. Eventually about 120 000 "persons of Japanese ancestry, both alien and non-alien" [14] were removed to conditions that have been compared to concentration camps [3].

[7]In total contrast to this, there were some suggestions during the panel discussion that a 'benign government' should be allowed to make this choice on behalf of citizens. It is not possible here to deal in full with Rawls's argument to show why such a just government would not be able to decide in favour of decreasing personal privacy for national security. In addition to Rawls's argument one also needs to consider the concept of 'benign government'. I suggest that the notion of a 'benign government' should not influence the decision on whether to decrease personal privacy, for reasons that include the fact that governments consist of politicians who often have to balance conflicting interests – and what is benign for one interest is not necessarily benign for another. (I also accept the general scepticism about politicians embodied by the remark of Karl Kraus: "Wars start when politicians lie to journalists and then believe what they read in the newspapers" [2, p. 120].)

vate, and what information – even though it is associated with an individual – may be considered public. Given the global nature of many IT solutions (and the cultural diversity of people affected by seemingly local IT applications), it makes sense to consider all information about an individual as potentially private.

Finally I will argue that, while societal protection of privacy is important, such protection is insufficient on its own. This motivates the need for technical solutions for privacy protection in addition to enhancing societal protection. Despite society's general acceptance of privacy principles, whether they are expressed as laws or not, one does not need to look far for examples of cases where privacy has been violated. Such violations range from 'innocent' gossip through cases where credit card numbers have been sold to even more serious cases. In one recent case a South African web service provider, Easyinfo, published the names, numbers, residential and postal addresses of many (most?) South African telephone subscribers. According to reports unlisted numbers were included [10]. Eventually Telkom (the South African telecommunications provider) persuaded Easyinfo to stop their service. The case received wide media coverage – possibly because "the home numbers of several high-profile politicians, businessmen, artists, journalists and media personalities" [10] were available on the site. While it is not too difficult to have one's number changed after such an infringement, it is not so easy to get a new home address to foil those parties who have obtained one's address while it was available on the Internet. Hence my contention that it is hard to regain privacy.

In the Easyinfo case, publication was stopped – presumably because of the number of people involved and the 'importance' of some of those affected. However, when only a few 'ordinary' people are involved, it seems that it may be much harder to try to rectify the matter. In the field of computer security, medical information of patients is widely used as an example of information that needs to be protected. And HIV status is often the paradigm case of information that needs the utmost protection. In March 2002 a South African politician's biography [9] was published that contained the HIV status of (at least) four HIV-positive people who did not want their HIV status made public.[8] Despite the patients being assisted from April 2002 by various parties (including the South African Human Rights Commission) the book, with the patients' name are still widely available at book shops in South Africa at the time of writing (September 2002).[9] Even though this case is not related to IT, it clearly illustrates that, unless you have the stature or personal legal machinery to act on privacy violations, after the fact complaints about privacy violations

[8]Outside their community the names of those whose HIV status were revealed will probably be just names; they were not even considered important enough to record their names in the index of the book...

[9]Arguments in the case dealt with aspects such as exactly who made the patients' names known first.

are unlikely to be effective – again supporting my contention that technical solutions should be developed to protect privacy before violations occur.

4. Bhavani Thuraisingham's Position

There has been much interest recently on using data mining for counterterrorism applications. For example, data mining can be used to detect unusual patterns, terrorist activities and fraudulent behavior. While all of these applications of the web and data mining can benefit humans, there is also a dangerous side to these technologies, since it could be a serious threat to the security and privacy of individuals. This is because data mining tools are available on the web and even naive users can apply these tools to extract information from the data stored on the web and consequently violate the privacy of the various individuals.

Privacy is getting more attention partly because of counterterrorism and national security. Data mining techniques such as classification, clustering, and associations can help to build terrorist profiles and identify potential terrorists. However, this also means that we have to gather all kinds of information about people events and entities. This means that there is a threat to privacy.

One of the challenges to securing databases is the inference problem. Inference is the process of users posing queries and deducing unauthorized information from the legitimate responses that they receive. This problem has been discussed quite a lot over the past two decades. However, data mining makes this problem worse. Users now have sophisticated tools that they can use to get data and deduce patterns that could be sensitive. Without these data mining tools, users would have to be fairly sophisticated in their reasoning to be able to deduce information from posing queries to the databases. That is, data mining tools make the inference problem quite dangerous.

Data mining approaches such as web mining also seriously compromise the privacy of the individuals. One can have all kinds of information about various individuals in a short space of time through browsing the web. Security for digital libraries, Internet databases, and electronic commerce is a subject of much research. Data mining and web mining make this problem even more dangerous. Therefore, protecting the privacy of the individuals is also a major consideration.

4.1 Data Mining for Counterterrorism

Data mining is the process of posing queries and extracting information often previously unknown from large quantities of data using mathematical, statistical reasoning and machine learning techniques. As mentioned earlier, there has been much interest in applying data mining for counterterrorism. By counterterrorism we mean protecting the infrastructures, people, and comput-

ers. Terrorism also includes bioterrorism and cyberterrorism. Data mining can help build profiles of potential terrorists and detect suspicious behavior.

To effectively carry out data mining we need good data. That is, we need to gather lots of data about people, events and entities. Furthermore data mining may give many spurious results. One needs to go through the data and extract often previously unknown patterns. This means that there could be false positives as well as false negatives.

False positives could cause serious violations to privacy and civil liberties. For example, just because John comes from country X and he is of a certain religion and he has associated with someone who is known to be a terrorist does not necessarily mean that John is a terrorist. However the data mining tool may determine that John is a potential terrorist. As a result John could be interrogated and even arrested. This is a serious violation to John's civil liberty. However data mining has also shown to be immensely useful in detecting hidden patterns and trends. That is, most of the time, the data mining tools could give out useful and accurate information. That is, but not carrying out data mining, we could loose valuable information about potential terrorist activities. The challenge is to develop good data mining techniques so that accurate results are obtained.

4.2 Privacy Issues

At the IFIP WG 11.3 Conference on Database Security in 1997, the group began discussions on privacy issues and the role of web, data mining, and data warehousing. This discussion continued at the IFIP WG 11.3 conference in 1998 and it was felt that IFIP WG 11.3 should monitor the developments made by the security working group of the world wide web consortium. The discussions included those based on technical, social, and political aspects. However it was the July 2002 meeting of IFIP WG 11.3 that resulted in much interest in national security vs. privacy.

First of all, with the World Wide Web, there is now an abundance of information about individuals that one can obtain within seconds. This information could be obtained through mining or just from information retrieval. Therefore, one needs to enforce controls on databases and data mining tools. This is a very difficult problem especially with respect to data mining, as we have seen in the previous section. In summary, one needs to develop techniques to prevent users from mining and extracting information from the data whether they are on the web or on servers. However, mining is a very important technology for numerous applications and it can help users to get the right information at the right time. Furthermore mining can also extract patterns previously unknown. The challenge is not to use information inappropriately. For example, based on information about a person, an insurance company could deny insur-

ance or a loan agency could deny loans. In many cases these denials may not be legitimate. Therefore, information providers have to be very careful in what they release. Also, data mining researchers have to ensure that security aspects are addressed.

Next, let us examine the social aspects. In most cultures, privacy of the individuals is important. However, there are certain cultures where it is impossible to ensure privacy. These could be related to political or technological issues or the fact that people have been brought up believing that privacy is not critical. There are places where people divulge their salaries without thinking twice about it, but in many countries, salaries are very private and sensitive. It is not easy to change cultures overnight, and in many cases you do not want to change them, as preserving cultures is very important. So what overall effect does this have on data mining and privacy issues? We do not have an answer to this yet as we are only beginning to look into it.

Next, let us examine the political and legal aspects. We include policies and procedures under this. What sort of security controls should one enforce for the web? Should these security policies be mandated or should they be discretionary? What are the consequences of violating the security policies? Who should be administering these policies and managing and implementing them? How is data mining on the web impacted? Can one control how data is mined on the web? Once we have made technological advances on security and data mining, can we enforce security controls on data mining tools? How is information transferred between countries? Again we have no answers to these questions. We have, however, begun discussions. Note that some of the issues we have discussed are related to privacy and data mining, and some others are related to just privacy in general.

We have raised some interesting questions on privacy issues and data mining as well as privacy in general. As mentioned earlier, data mining is a threat to privacy. The challenge is on protecting the privacy but at the same time not losing all the great benefits of data mining. At the 1998 knowledge discovery in database conference, there was an interesting panel on the privacy issues for web mining. It appears that the data mining as well as the security communities are interested about security and privacy issues.

4.3 Civil Liberties vs. National Security

Civil Liberties are about protecting the rights of the individuals whether they are privacy rights, human rights or civil rights. There are various civil liberties unions and laws protecting these rights (see, e.g., www.aclu.org).

There has been much debate recently among the counterterrorism experts, civil liberties unions and human tights lawyers about the privacy of individuals. That is, gathering information about people, mining information about

people, conduction surveillance activities and examining say e-mail messages and phone conversations are all threats to privacy and civil liberties. However, what are the alternatives if we are to combat terrorism effectively? Today we do not have any effective solutions. Do we wait until privacy violation occurs and then prosecute or do we wait until national security threats occur and then gather information? What is more important? Protecting nations from terrorist attacks or protecting the privacy of individual? This is one if the major challenges faced by technologists, sociologists and lawyers. That is, how can we have privacy but at the same time ensure the safety of nations? What should we be sacrificing?

I have served on several panels on national security, database technologies and privacy. I have heard audiences say that if they can be guaranteed that there is absolute national security, then they would not mind sacrificing privacy. However they would not want to sacrifice privacy for a false sense of national security. On the other hand I have heard people say that some security is better than nothing. Therefore, even if one cannot guarantee national security, if some security is provided, then sacrificing privacy is not an issue. I have also heard from human rights lawyers about occurrences of privacy violation under the pretext of national security. Some others are nervous that all the information gathered about individual may get into the wrong hands one day and then things could be disastrous.

While we have no solutions today, we will certainly hear more about it in coming months and years. The question is, if we assume that there will be no misuse of information, then should we sacrifice privacy for security? Is it reasonable to make such assumption? On the other hand should national security be of utmost importance and we prosecute those who have violated privacy on a case by case basis. Do we have adequate laws? We have no answers, just questions at this point.

4.4 Summary

This contribution is devoted to the important area of security and privacy related to web as well as privacy issues for data mining. While there have been efforts on applying data mining for handling national security problems such as detecting and preventing terrorism as well as intrusion detection, there are also negative effects of data mining. In particular, we discussed the inference problem that can result due to mining as well as ways of compromising privacy especially due to web data access.

While little work has been reported on security and privacy issues for web and data mining, we are moving in the right direction. There is increasing awareness of the problems and groups such as the IFIP working group in database security are making this a priority. As research initiatives are started

in this area, we can expect some progress to be made. Note that there are also social and political aspects to consider. However, as web becomes more and more sophisticated, there is also the potential for more and more threats. Therefore we have to be ever vigilant and continue to investigate, design and implement various security and privacy measures for the web.

5. Eleanor Sharpston's Position

This presentation is composed – in true Descartian fashion – of two parts. First, I set out some points of principle (depending on one's perspective, either simple self-evident truths or dangerous liberal assertions) which are worth repeating in the current climate of uncertainty and which, in my view, must inform any valid debate about the extent to which technology should be placed at the service of the State to promote national security interests even though this may be at the expense of individual privacy. The second part analyses these issues from the perspective of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the "ECHR").

5.1 Part I

Strange though this may sound coming from a lawyer, there are clear limitations to what law can do. Law is not a magic box of tricks. To highlight a few (obvious) points: the rules law lays down reflect the choices made by society, there are always issues about enforcement, and there are almost always technical ways of "getting round" the law. However, law does have an essential part to play in arriving at an ethically justifiable society.

At best, law governs how "our side" uses technology. It has no control over how "the other side" uses it. That raises difficult philosophical issues. Can a "civilised" society permit itself to fight as dirty as its "sub- human" opponents? Try asking that question about the US response to September 11 and its aftermath; about Israel confronted by Palestinian suicide bombers; or about the proportionality (or otherwise) of the British army's response, on "Bloody Sunday" in [London]Derry, to years of IRA activity in Northern Ireland. These three emotional examples are deliberately juxtaposed to act as an antidote to our natural instinct to identify with our favourite cause. If you answer even one example by querying the appropriateness of a "no-rules" reaction by government, you are endorsing the principle that a civilised society plays by higher ethical rules than its opponents even if it is less "efficient" for it to do so.

Human rights are not just there to protect the people we *like* (usually, they won't need protecting). They are there, precisely, to protect people we don't like – the marginalized, the ones who hold different (and objectionable) views, the ones who disgust us by following different (and objectionable) lifestyles and practices.

Turning to the specific issue of privacy versus national security, clearly there are two extremes (absolute privacy at the expense of any concern for national security, and vice versa). One would expect the debate to focus on where, between those two extremes, the balance should be struck. Operating within this spectrum are the various players: governments, individuals, the international community and (Swiss mercenary-like) the lawyers.

On the basis of over 20 years' experience litigating against and on behalf of the State, I do not believe that there is such a thing as a "benevolent government." All governments are concerned to exercise and retain power. All governments cut corners when it suits them – that is, when they perceive an overriding need to set aside some tedious small rule. The value of an enduring, overriding legal structure is that it enables one to test, objectively, the weight and credibility of a government's claim, "This is a crisis – so let's change all the rules." Whether the crisis invoked is September 11 or drug trafficking, civilised societies use established structures to assess whether the government's proposed interference with civil liberties in this particular case is justified, whether the necessary procedural guarantees are in place, whether there is access to the courts and – above all – whether there is some continuing independent verification of the extent, duration and legitimacy of the reduction of individual liberty.

No nation state, however big and powerful, has a legitimate right to ignore international structures for dispute resolution and to "go it alone" with its chosen (solo) solution. It *can*, of course, do so; but only at the cost of forfeiting pluralist democratic support for its actions from the international community.

5.2 Part II

Against that background, I listened to the proposed list of types of data that "should" be "mined" in order to put together profiles for use in anti-terrorist surveillance and interception work. I cannot conceive of circumstances in which I would accept that list at face value. My own (admittedly limited) experience in handling sensitive material convinces me that a lot is about hoping that one has drawn the right inferences from individual pieces of information. The inferences may not be correct (or, of course, there may simply be data corruption – the individual data items may not all relate to the *same* "John Smith"). Whilst there is indubitably *a* need for access to *some* information, agreeing to unrestricted government use of all data on that list involves a massive violation of individual privacy. How, then, to analyse whether the need for access outweighs the privacy rights?

The structure of Article 8 ECHR (the "right to privacy" article of the Convention) has nothing particularly magic about it (similar provisions can be found in other international instruments), but it will serve as a paradigm for

analysis. Article 8(1) formulates the right to privacy: "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8(2) then gives the State *qualified permission* to interfere with that right. Interference is only permissible if it satisfies specific criteria, each of which have been sharpened and defined by the case law of the Strasbourg court. Interference must be "in accordance with the law." It must be "necessary in a democratic society." It must be for one of the public interests specified in an exhaustive list (national security is the first entry: the list also includes "public safety," "the prevention of disorder or crime" and "the protection of the rights and freedoms of others)." Finally, as the case law makes clear, the interference must correspond to a "pressing social need" and be "proportionate" to the legitimate aim pursued – no sledgehammers to shatter nuts when a nutcracker will do the job. The individual items in the proposed list of types of data would need to be examined, together with the nature and extent of their intended use and the proposed safeguards (procedural guarantees, independent review), and *individually justified* in order to satisfy the Article 8 tests.

I add that the ECHR also contains limited provision (in Article 15 - derogation "in time of *war or other public emergency threatening the life of the nation*") enabling a contracting State to "take measures derogating from its obligations under this Convention to the *extent strictly required* by the exigencies of the situation, *provided* that such measures are *not inconsistent* with its *other obligations under international law"* (emphasis added). Certain articles cannot be derogated from even under such circumstances. Article 15 also contains a control mechanism to prevent abuse of the power to derogate.

If a civilised democracy *cannot* manage to justify its interference with privacy within that framework, my own view is that it has no legitimacy in claiming that it is nevertheless "entitled" to interfere with individual rights to privacy.

Acknowledgments

The work of Pierangela Samarati has been supported in part by the European Commission within the Fifth (EC) Framework Programme under the Roadmap for Advanced Research in Privacy and Identity Management (RAPID) Project, Contract IST-2001-38310.

References

[1] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati and F. Violante, A reputation-based approach for choosing reliable resources in peer-to-peer networks, *Proceedings of the Ninth ACM Conference on Computer and Communications Security*, 2002.

[2] W. Gratzer, *The Undergrowth of Science: Delusion, Self-Deception and Human Frailty*, Oxford University Press, 2000.

[3] J. Hirabayashi, Concentration camp or relocation center: What's in a name? *Japanese American National Museum's Quarterly*, vol. 9(3), 1994.

[4] M. Lessnoff (ed.), *Social Contract Theory*, Basil Blackwell, 1990.

[5] N. Mandela, *Long Walk to Freedom*, Abacus, 1994.

[6] A. Margalit, *The Decent Society*, Harvard University Press, 1996.

[7] C. Pfleeger, *Security in Computing*, Prentice-Hall, 1989.

[8] P. Samarati, Protecting respondents' privacy in microdata release, *IEEE Transactions on Knowledge and Data Engineering*, vol. 13(6), pp. 1010-1017, 2001.

[9] C. Smith, *Patricia de Lille*, Spearhead, 2002.

[10] The Star, Easyinfo's number is up after Telkom deal (www.iol.co.za /index.php?set_id=1&click_id=13&art_id=ct20020219235905891T42544), February 19, 2002.

[11] B. Thuraisingham, S. Jajodia, P. Samarati, J. Dobson and M. Olivier, Privacy issues in the world-wide web and data mining: Panel discussion, in S. Jajodia (ed.), *Database Security XII - Status and Prospects*, Kluwer, 1999.

[12] B. Thuraisingham, S. Jajodia, P. Samarati and M. Olivier, Security and privacy issues for the world-wide web: Panel discussion, in S. Jajodia (ed.), *Database Security XII: Status and Prospects*, Kluwer, pp. 269-284, 1999.

[13] Harry S. Truman Presidential Library, The War Relocation Authority and the incarceration of Japanese-Americans during WWII (www.trumanlibrary.org/whistlestop/study_collections/japanese_internment /1942.htm), 2001.

[14] Western Defence Command and Fourth Army Wartime Civil Control Administration, Presidio of San Francisco, California, Instructions to all persons of Japanese ancestry, *Civil Exclusion Order 92*, US Army, 1942.

Appendix: A

A shortlist of relevant/interesting/thought-provoking decisions of the European Court of Human Rights (there is plenty more case law):

- **McCann v. United Kingdom** (1996) 21 EHRR 97 (IRA "active service unit" killed by SAS whilst reconnoitring to plant a bomb in Gibraltar: held, the UK had violated the right to life in Article 2 ECHR)
- **Ireland v. United Kingdom** (1978) 2 EHRR 25 (five interrogation techniques used by the British authorities on terrorist suspects in Northern Ireland held to be inhuman treatment violating Article 3 ECHR; careful distinctions drawn between torture, inhuman treatment and degrading treatment; UK gave solemn undertaking that the authorities would no longer use those five techniques)
- **Malone v. United Kingdom** (1985) 7 EHRR 14 (telephone surveillance under Home Secretary's warrant: obscurity and uncertainty of domestic legal provisions led to finding that Article 8(1) violated)
- **Harman and Hewitt v. United Kingdom** (1992) 14 EHRR 657 (Commission decision) (collection and retention of information by MI5 not "in accordance with law," therefore violation of Article 8(1); Government arrived at "friendly settlement")
- Finally, note the admonitory words of the European Court of Human Rights in **Klass v. Germany** (1978) 2 EHRR 214 (German State powers to open mail and listen to telephone conversations in order to protect against, *inter alia*, "imminent dangers" threatening the "free democratic constitutional order" and "the existence or the security of the State": because safeguards were detailed and effective, no violation of the Convention was found): "the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8(2), are not to be exceeded."

Article 15 ECHR

The Article 15 derogation power does *not* include power to derogate from the following articles:

- Article 2 (right to life) "except in respect of deaths arising from lawful acts of war;"
- Article 3 (prohibition of torture and of inhuman or degrading treatment or punishment);
- Article 4, first sentence (prohibition of slavery and servitude);
- Article 7 (prohibition on retroactive criminalisation of conduct and 7 consequent punishment of conduct ("punishment without law"))