Volume 6 (2): 119–134: 1477-3708
DOI: 10.1177/1477370808100541

Los Angeles, London, New Delhi, Singapore and Washington DC
www.sagepublications.com

European Journal of Criminology

ARTICLES

Terrorism and the Proportionality of Internet Surveillance

Ian Brown
University of Oxford, UK

Douwe Korff
London Metropolitan University, UK

ABSTRACT

As the Internet has become a mainstream communications mechanism, law enforcement and intelligence agencies have developed new surveillance capabilities and been given new legal powers to monitor its users. These capabilities have been particularly targeted toward terrorism suspects and organizations that have been observed using the Internet for communication, propaganda, research, planning, publicity, fundraising and creating a distributed sense of community. Policing has become increasingly pre-emptive, with a range of activities criminalized as 'supporting' or 'apologizing for' terrorism. The privacy and non-discrimination rights that are core to the European legal framework are being challenged by the increased surveillance and profiling of terrorism suspects. We argue that their disproportionate nature is problematic for democracy and the rule of law, and will lead to practical difficulties for cross-border cooperation between law enforcement agencies.

KEY WORDS

Correspondence / Electronic Communications / Human Rights / Privacy / Surveillance.

Introduction

Over the last 15 years the Internet has developed from a specialist network of academic researchers into a mainstream communications mechanism. Around 60 per cent of the UK population are now regular Internet users, most commonly for email and Web browsing (Dutton and Helsper 2007).

As might be expected of any such widespread technology, law enforcement agencies have paid increasing attention to the use of the Internet for criminal purposes, especially by terrorism suspects. Terrorist groups such as Hezbollah have been observed using the Internet for communication, propaganda, research, planning, publicity, fundraising and creating a distributed sense of community. Email and Web discussion forums have been used to plan operations, while websites are commonly used to bypass media editorial controls and communicate directly with groups' supporters and potential recruits (Bird 2006; Labi 2006).

In response to this activity, policing and intelligence agencies have developed new capabilities and successfully lobbied for new legal powers to put Internet users under surveillance. These have included requirements for Internet service providers (ISPs) to facilitate wiretaps and to store information about their customers' communications and Web browsing activities (Brown and Korff 2004; Schjolberg 2007). However, these new powers have caused significant concern that the private lives of Internet users with no connection to terrorism or serious crime are being disproportionately invaded, and are one reason that UK Information Commissioner Richard Thomas believes we are 'sleepwalking into a surveillance society' (Ford 2004).

The right to privacy relates to the right to respect for private life, guaranteed by Article 8 of the European Convention on Human Rights (ECHR), but is also shorthand for a more specific right, usually referred to in terms of 'data protection'. This is increasingly recognized as a right *sui generis* (e.g. in Article 8 of the EU Charter on Fundamental Rights) and is not only concerned with protecting individuals from intrusions into their privacy or private life, but more broadly against the improper collecting, storing, sharing and use of their data. It addresses the central issue in the 'information society' of the extent of control by 'data controllers' over individuals – tellingly referred to as 'data subjects' – through possession of their data.

The proportionality of Internet surveillance touches on fundamental values of a democratic society, raising serious constitutional questions in many states. However, it relates to a phenomenon – terrorism – in response to which states feel obliged to take the most drastic action, if needs be in derogation of their usual human rights obligations applicable in 'ordinary' times. Yet terrorism (however defined) is not a passing phenomenon. While wars or other public emergencies generally have a more-or-less clear end (even if this can be much-delayed), there is no end in sight in the fight against terrorism. Even at the national level, anti-terrorism legislation tends to become semi-permanent (Walker and Akdeniz 2003).

Terrorist use of the Internet

While much media attention has focused on the possibilities of dramatic 'cyber-terrorism' and even digital 'Pearl Harbours', the reality of terrorist use of the Internet is more prosaic (Brown 2007). Researchers have found that online terrorist activity is most commonly for the purposes of communication, propaganda, research, planning, publicity, fundraising and creating a distributed sense of community (Bird 2006).

Terrorists communicate online for the purposes of bonding, social interaction, planning and executing acts. Email is their main tool but voice over Internet protocol (VoIP) is also used, both largely to support existing relationships. Blogs, chatrooms and message boards (sometimes password protected) are also used to reach a wider audience, particularly potential supporters and recruits (Ryan 2007). The use of encryption to scramble the contents of messages is no more prevalent among terrorists than the general population – not least because it might make messages stand out. The use of steganography to disguise the existence of messages is discussed more by intelligence services than used by terrorists because it is technically challenging and hence less appealing (Bird 2006).

Websites often contain valuable technical information (which vary in quality) such as maps, plans, how to construct suicide belts or extract toxins, conspiracy theories, militant texts, Qu'ranic interpretations and detailed anti-terrorist programmes. The majority of 'recipes' for chemical and biological weapons available online are of poor quality and are unlikely to lead to the production of usable weapons (Stenersen 2007). However, the US Army recently had to remind soldiers of the operational security issues inherent in blogging from the front-line (US Army 2005); one prominent online terrorist wrote in 2004: 'I'm looking for soldier footages from within US bases etc.' (Labi 2006).

Terrorist websites make strong efforts to increase public sympathy for their cause and sow doubts about the validity of the status quo. The Internet is an ideal propaganda tool and most extremist groups therefore have a Web presence. Sites are cheap to produce while looking professional, adding validity and legitimacy to a cause. It is relatively easy for extremists to use multimedia, which appeals to the young and less literate. To get press coverage, groups previously had to attract the attention of journalists and even then could be pushed out by a competing story or editor. Groups can now bypass these gatekeepers and communicate directly with supporters and potential recruits. Al-Qaeda publishes pictures of attacks and lists of 'martyrs,' and has a seamless public relations effort with its own media agency. Sites are monitored by journalists, who replay the most shocking footage in

the mainstream media – including videos such as the beheading of American businessman Nicholas Berg. Sites are also a route for disinformation and psychological operations such as the posting of casualty figures and attack warnings (Bird 2006). In contrast, earlier terrorist groups such as ETA and the IRA had to rely on word of mouth and local newspapers.

Terrorist groups monitor online forums for potential new recruits ('armchair jihadis'), who will be contacted directly by an ideologue (an 'international dating service') who will radicalize and train the recruit. Once fully prepared they are passed on to an operational leader, who will provide tactical training in specific skills such as counter-surveillance, target selection or bombmaking. The armchair jihadi can now form a cell offline, and further support will come on the ground (Shahar 2007).

Websites and forums are also used to give terrorists and their supporters a sense of belonging (Labi 2006). Sites reassure members they are not misfits or loners. Sites have their own iconography – horses, flags and sunrises are the online equivalents of scarves. Hezbollah and Hamas produce souvenirs featuring logos. While local terrorist motivations (e.g. in Chechnya, Afghanistan, Saudi Arabia) are very different, their websites give them a global jihad spin. The youngest, least educated and literate (especially religious converts) are particularly strongly influenced by multimedia propaganda (Bird 2006). The Internet is providing a social networking function for terrorists, allowing them to normalize their behaviour and to develop a sense of persecution.

The Internet has also changed the way global terrorism functions. Groups can now be more geographically dispersed and non-hierarchical. Such networks have been proven capable of defeating much more powerful hierarchies. 'Leaderless resistance', which originated in printed media, can now work much more effectively. Terrorist organizations can flourish without state sponsors, who are vulnerable to threats of retaliation. They are instead sponsored by sub-state entities that operate more like corporations (Shahar 2007).

Terrorist use of new technologies provides new opportunities for intelligence gathering and disruption of operations by intelligence agencies. They can use active and passive attacks (e.g. viruses and surveillance/traffic analysis) on terrorist computers to gather address books, cookies, passwords and similar information. Counter-terrorist operations include the use of black propaganda to destroy trust. If agencies can identify and 'take out' purveyors of good technical information, they can flood channels with misinformation and leave the less informed to propagate bad information. At the same time they gather intelligence on participants, organizations and their modus operandi. Most ideological debate takes place on open

recognized sites, including senior participants, which allows up-and-coming leaders to be identified (Shahar 2007).

Jihadi websites provide much information about their organizations, including core beliefs; ideological divisions; ultimate goals and overall game plan; methods proposed to reach these goals; who makes decisions and how these are made. They often detail ideological splits and identify clerics who will dispute Qu'ranic interpretations who can be co-opted, intimidated or killed, providing a mechanism for intelligence agencies to challenge terror groups' legitimacy and siphon off recruits. Movements often split over theological (not tactical) disagreements.

Tactical discussion and training manuals show favoured tactics and weapons and assumptions on effectiveness, into which disinformation can be fed. Terror groups' own propaganda and recruitment messages can be used against them and to inoculate potential recruits. Furthermore, the structure of websites mimics the structure of organizations – Hezbollah's is very top-down with instructions for supporters, whereas Al-Qaeda sites are very interactive and non-hierarchical (Shahar 2007).

Surveillance, profiling and data sharing

Alongside the development in communications technology that has driven the growth of the Internet, we continue to see exponential increases in computing capability and data storage capacity. Processing power has doubled roughly every two years, increasing a million-fold since 1965. Bandwidth and storage capacity are growing even faster, doubling every 12 months (Brown and Korff 2004: 9–16).

New surveillance technologies exploiting these capabilities include mechanisms to monitor, screen and analyse records of billions of telephone and email communications; 'bugs' and tracing technologies that can access the geographical position of mobile phones and act as a remote listening device; and hard-to-detect (even with anti-virus tools) 'spyware', surreptitiously installed on a suspect's computer by the authorities, that can remotely and secretly monitor a suspect's online activities, passwords and email, and even the computer's camera and microphone. Surveillance computers do not just observe: they direct the attention of police and other authorities to 'targets' identified by algorithm (Brown and Korff 2004).

There has been a commensurate expansion in 'dataveillance': the monitoring of the 'data trails' left by individuals in numerous transactions, through access to communications databases containing such trails. The EU's 2006 Data Retention Directive stipulates the mandatory retention time, beyond the period for which they may be stored under 'normal' data

protection rules, of electronic communications data by providers of communications services. This data includes records of telephone numbers dialled and email senders and recipients – but not the content of calls or messages. The rules on access to communications data and on data retention are opaque and do not guarantee that data on innocent individuals will not be obtained and held by law enforcement authorities, or used in 'profiling' (as discussed later). The picture of an individual that can be built up from communications data is immensely detailed. There is little room for privacy when state investigators can see with whom we communicate, what we read and watch online, and where we travel via mobile phone use.

Data gathered by law enforcement agencies are now available to be shared across Europe under the principle of 'availability', defined in the 'Hague Programme' of the European Union as follows:

> With effect from 1 January 2008 the exchange of … information should be governed by conditions set out below with regard to the principle of availability, which means that, throughout the [European] Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State.
>
> The methods of exchange of information should make full use of new technology and must be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (on-line) access. (European Commission 2005)

This allows data sharing and free access without any of the usual 'obstacles' contained in the traditional instruments for transnational cooperation between law enforcement agencies. These include the 1959 (Council of Europe) European Convention on Mutual Assistance in Criminal Matters and its two additional protocols and the EU Convention on Mutual Assistance in Criminal Matters of 2000 (which builds on the Council of Europe Convention), with its additional protocol, which both came into effect in 2005. The procedures under these treaties take time and, more importantly, involve formal requests for specified information and often require judicial authorization.[1]

[1] To see those requirements as 'problems' and 'obstacles' is to ignore that they constitute fundamental safeguards for the individual. As the European data protection authorities put it in their statement from a recent meeting: 'In view of the increasing use of availability of information as a concept for improving the fight against serious crime and the use of this concept both on a national level and between Member States, the lack of a harmonized and high level of data protection regime in the Union creates a situation in which the fundamental right of protection of personal data is not sufficiently guaranteed anymore' (Article 29 Working Party 2007).

Law enforcement agencies in Europe now commonly rely on the use of 'profiles' to target suspects. Such profiles are increasingly created not by any one national police force (and/or intelligence agency), but as part of international (in particular intra-EU) co-operation. In order to 'facilitate targeted searches for would-be terrorists' member states gather data from registers of residents, foreigners, university students and similar information sources. Their aim is to match such data against 'physical, psychological or behavioural' characteristics that are thought by law enforcement agencies to indicate a high probability of terrorist activity (Privacy International 2005).

The police and intelligence agencies do not just search these massive data resources in order to find previously identified suspects of specific (terrorist or other) offences. Increasingly, they 'trawl' through such databases in order to 'match' all those in those databases against a pre-determined (but dynamically updated) 'profile'. Moreover, such searches are commonly 'intelligence-led' – based on secret, unchallengeable information; and carried out as part of European (rather than just national) policies. Profiles created in this manner suffer from built-in biases of which even software producers are often unaware, or that may only become apparent when these programs are used in practice – and then only if their operation is adequately monitored for such distortions (Brown and Korff 2004).

Many of these technologies pose inherent threats to privacy: they allow the state extremely close control over citizens' lives. But they are not infallible – on the contrary, these technologies are subject to serious, inherent limitations and biases. 'Profiling' and 'data mining' may seem to work up to a point, but they *inevitably* lead to actions against very large numbers of innocent people, on a scale that is both unacceptable in a democratic society and which renders the 'trawl' useless. Attempts to identify very rare incidents or targets from a very large data set are highly likely to result in unacceptably large numbers of 'false positives' (identifying innocent people as suspects) or 'false negatives' (not identifying real criminals or terrorists). This is referred to scientifically as the 'base-rate fallacy'; colloquially, as: 'if you are looking for a needle in a haystack, it doesn't help to throw more hay on the stack' (Schneier 2006). A recent US National Research Council (2008: 4) report concluded: 'there is not a consensus within the relevant scientific community nor on the committee regarding whether any behavioral surveillance or physiological monitoring techniques are ready for use at all in the counterterrorist context given the present state of the science'.

The changing role of the police

In many European countries the police are increasingly seen as part of a wider 'full societal alliance', implementing overall state policies. This inevitably widens the area in which the state feels justified to take action – including intrusive or punitive action – against people who have not (yet) committed any crime. In respect of offences such as narcotics possession and prostitution, this may not necessarily involve use of the criminal law. However in the area of terrorism the aim is to prevent *possible* crimes by people who *may* commit them. Law enforcement agencies have lobbied for powers to arrest and detain people who they think may be likely to commit crimes, or at least terrorist crimes (Cobler 1976). Indeed, preventive detention of such suspects is already a feature of the UK's Anti-Terrorism, Crime and Security Act 2001.

The definitions of the crimes in question – or of more general 'grounds for suspicion' (*Verdachtsmomente*) that are felt to justify police action – are becoming increasingly vague. In spite of the great attention given by states to terrorism, especially after 9/11, even this concept is still largely undefined (Bowring 2006: 78). Specifically, neither the European Convention on the Suppression of Terrorism 1977, nor the UN International Convention for the Suppression of Terrorist Bombings 1999 defines the word 'terrorism'.[2] Nor has the UN Security Council (or, for that matter, the EU) adopted a definition, in spite of the fact that it mandates punitive actions against suspected 'terrorists'. Lord Carlile, the UK's Independent Reviewer of Terrorism Legislation, concluded that: 'There is no universally accepted definition of terrorism. It remains the subject of continuing debate in international bodies' (2007: 3).

Apart from 'terrorism', many states have now criminalized acting for 'terrorist purposes', 'supporting terrorism', 'possession of materials that may be of use to terrorists' (irrespective of an intention to actually provide

[2] One of the problems with finding an acceptable definition is the difficult relationship between terrorism, 'political offences' and liberation struggles. There is a tendency in various instruments to list certain offences and to then declare that they will constitute terrorism if they are carried out for broadly political motives. E.g. one could read a definition into the European Convention on the Suppression of Terrorism, if one were to say that terrorism covers the offences listed in Articles 1 and 2 of that Convention, when 'inspired by political motives': in a way, the Convention tries to overcome certain restrictions on international co-operation in respect of 'political' crimes by excluding the relevant offences from that definition, even if carried out for political reasons. See also Article 3(1) of Framework Decision 2002/475/JHA. But there are also problems with defining terrorism purely by reference to such motives, or to certain types of offences. Note for instance that the 2005 Council of Europe Convention includes the crime of 'public provocation' of terrorism.

them to terrorists), 'apologising for terrorism' and even 'extremism' (Hirsch 2007). Punitive measures are increasingly envisaged against people perceived (defined?) to be 'enemies of the State' or of 'our democratic legal order' – even if their opinions and actions (although perhaps repulsive) would in the past not have been considered to constitute criminal offences. The widening of the police remit to include such matters, risks penalizing people for their views and beliefs rather than for actual acts against society.

The current focus on trying to prevent individuals (in particular, young Muslims) from being drawn into 'extremism' also fits into these wider developments. Actions against individuals deemed to be suspicious because they fit a certain stereotype or belong to a specific group are almost certain to lead to discrimination against such minority groups.[3] The fact that a supposedly sophisticated computer-generated algorithm replaces a coarse stereotype does little to prevent this. By being incomprehensible even to those that rely on it, and effectively unchallengeable by those that are targeted, it aggravates the risk of discrimination.

A further major change in the policing environment concerns the relationship between the police and intelligence agencies. The former are working increasingly closely with, and relying on information obtained and passed on by, the latter. The police are also adopting many of the techniques and technologies of the intelligence agencies. As a result, the basis for police 'interest' in a person, and the nature of the evidence against that person, are hidden. This has a direct impact on the treatment of such a person, who is likely to be spied upon, harassed, arrested, denied a job or a research post (Institute for Race Relations 2004) – all without knowing why, or able to challenge the reasons for such actions (or without even being aware of them). The ever-closer relationship between the police and intelligence agencies undermines the fairness of trials against persons accused of being involved in organized crime or terrorism, in that courts increasingly allow effectively secret evidence and evidence from anonymous witnesses to form the basis for a conviction (Vervaele 2005).

Proportionality and the European legal framework

European privacy law is complex, developing under a range of separate (Council of Europe, Single Market and Third Pillar EU) instruments, often

[3] As they did for example, in the UK during the 1970s and 1980s through the use of the stopped under suspicion (or SUS) law. This allowed the stopping and searching of people on the subjective suspicion of individual police officers – powers which were used in a grossly discriminatory way before being finally repealed (but which are being brought back in new forms in recent anti-terrorism laws) (see Chapter 13 Cownie et al. 2007).

ad hoc, by different national and international (European) judicial and other bodies.

Data protection has been developed on the basis of Article 8 of the ECHR. Over the last decade the European Court of Human Rights has given strong recognition to data protection principles under this article, in particular in the cases of *Peck* v. *the UK* (concerning CCTV), *Amann* v. *Switzerland* (concerning telephone interception), *Rotaru* v. *Romania* (concerning secret service files) and *Copland* v. *the UK* (concerning the question of when the legal basis for processing of personal data can be considered to be adequate – to constitute 'law' – in terms of the ECHR).

Data protection is however also increasingly seen as a *sui generis* right, in particular in the EU Charter of Fundamental Rights, in which it is given a separate provision (Article 8). More specifically, the following general European data protection instruments have been developed:

- The 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol.
- Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (also referred to as the Directive on Privacy and Electronic Communications or DPEC).

Under these instruments, rules and guidelines have been issued that specifically relate to processing of personal data for law enforcement purposes. These include, in particular, Council of Europe Recommendation R(87)15 of the Committee of Ministers to Member States, *Regulating the Use of Personal Data in the Police Sector* (1987). This recommendation has become the effective standard on the issue: it is expressly referred to in various European police co-operation instruments, including the Schengen and Europol treaties and associated regulations, and is also regularly invoked in recommendations by the Parliamentary Assembly of the Council of Europe and its Committee of Ministers, by the Working Party, and the European Parliament.

The European Court of Justice (ECJ) in Luxembourg has also been strict in its application of data protection principles (derived from both the ECHR as reflected in 'general principles of Community law' and from the above EC directives); see in particular the cases of *Österreichischer Rundfunk* v. *Austria* and *Lindqvist* v. *Sweden*. It is clear from these cases that in the

view of the ECJ, data protection is a fundamental, constitutional issue that should be applied in accordance with the jurisprudence of the European Court of Human Rights. The ECJ has clearly endorsed, and adopted for itself, the typical, 'standard' approach to human rights developed by the Strasbourg Court – and follows this approach also and in particular in its assessment of cases relating to the Framework Directive.

In their judgments, the European Court of Human Rights and the European Court of Justice have developed a broad range of standards around data protection and law enforcement. They require a legal basis for any collection, storage, use, analysis, disclosure/sharing of personal data for law enforcement and anti-terrorist purposes – but a vague, broad general statutory basis is not sufficient. Such processing must be based on specific legal rules relating to the particular kind of processing operation in question. These rules must be binding, and they must lay down appropriate limits on the statutory powers such as a precise description of 'the kind of information that may be recorded', 'the categories of people against whom surveillance measures such as gathering and keeping information may be taken' and 'the circumstances in which such measures may be taken' (*Rotaru* vs. *Romania*). Legislation must include a clearly set out procedure to be followed for the authorization of such measures, limits on the storage of old information and on the time for which new information can be retained. It must also include explicit, detailed provision concerning the grounds on which files can be opened, the procedure to be followed for opening or accessing the files, the persons authorized to consult the files, the nature of the files and the use that may be made of the information in the files. Such rules can be set out in subsidiary rules or regulations – but in order to qualify as 'law' in Convention terms, they must be published.

In order to properly comply with the core 'purpose-specification and limitation' principle, it is not sufficient to specify that processing serves 'the police task' or even a specific police task (investigation and prosecution of crime; countering immediate threats; more controversially, 'prevention'). States must be as precise as possible. Personal data, collected for one specific police purpose (e.g. countering threats) can only be used for another specific purpose (e.g. investigating offences) if the data could have been independently collected for that second purpose. The police or other law enforcement agencies should never collect personal data 'just in case'.

The EC Data Protection Directive (Directive 95/46/EC) stipulates that if a person is subjected to a fully automated decision, the individual should (at least) have the right to know the logic involved in this decision, and measures should be taken to safeguard the individual's legitimate interests. The scope and application of this principle is still rather unclear, even in

the First Pillar. However, the underlying principle – that it would violate 'human identity', 'dignity' or 'personality' to treat anyone on that basis without stringent safeguards – must surely also be applied in the Third Pillar. This clearly has implications for the 'profiling' of terrorist suspects.

In addition, there must be strong 'safeguards established by law' that ensure 'appropriate [and effective] supervision of the relevant services' activities'. The judiciary should 'normally' carry out this supervision. There should otherwise be particularly strong alternative supervisory mechanisms, such as close parliamentary scrutiny. This requirement is part of the test of whether the legal rule in question has the appropriate quality. But the existence of such procedures is also essential in the assessment of compliance with Article 13 ECHR (the right to an effective remedy before a national authority). The European Court of Human Rights has confirmed that a remedy should be available to anyone with an 'arguable claim' of a violation of a Convention right: there is no need to show that an actual violation has occurred – which in the case of secret surveillance would put individuals in an impossible position.

It follows from the above that the collection of data on 'contacts and associates' (i.e. on persons not suspected of involvement in a specific crime or of posing a threat), the collection of information through intrusive, secret means (telephone tapping and email interception) and the use of 'profiling' techniques, and indeed 'preventive' policing generally, must be subject to a particularly strict 'necessity' and 'proportionality' test, and surrounded with particularly strong safeguards. 'Hard' (factual) and 'soft' (intelligence) data should be clearly distinguished, and data on different categories of data subjects (officially indicted persons, suspects, associates, incidental contacts, witnesses and victims, etc.) should be clearly distinguished. The nature of information and intelligence coming from private parties requires additional safeguards, inter alia in order to ensure the accuracy of this information since these are personal data that have been collected for commercial purposes in a commercial environment. Access should only be allowed on a case-by-case basis, for specified purposes and be under judicial control in the Member States.

Conclusion

States have a positive obligation to protect the life of their citizens (*Osman* v. *United Kingdom*). They are obliged to do all that could be reasonably expected of them to avoid a real and immediate risk to life of which they have or ought to have knowledge. In this sense, the right to security has long been 'codified' as a human right in the jurisprudence of the European Court

of Human Rights. This doctrine is equally applicable to life-threatening situations as a result of a terrorist threat. The preamble to the *Guidelines on Human Rights and the Fight Against Terrorism* that the Council of Europe's Committee of Ministers adopted on the of 11 July 2002 refers to 'the imperative duty of the States to protect their populations against possible terrorist acts' (Council of Europe 2002: 7). The same consideration can be found in the *Guidelines on the Protection of Victims of Terrorist Acts*, adopted by the Committee of Ministers on the 2 March 2005. However, in *Osman* the Court also stressed:

> the need to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice, including the guarantees contained in Article 5 and 8 of the Convention.

States thus have the difficult job of balancing competing human rights interests. They must protect their population against terrorist threats whilst safeguarding the fundamental rights of individuals, including persons suspected or convicted of terrorist activities.

Anti-terrorist and related policies have given an immense impetus to pre-existing developments in law enforcement surveillance of communications. These measures are often adopted on a temporary, emergency basis – but once introduced, become permanent and are extended into the general law. It is becoming less and less common for sunset clauses to be included in such legislation (Walker and Akdeniz 2003). These measures present a direct challenge to citizens' privacy rights as articulated in *Osman*.

Policing is being 'brought forward' to target not just criminal, but also more generally deviant behaviour. In the context of the fight against terrorism, this means individuals are targeted for being suspected 'extremists' or for being suspected of being 'opposed to our constitutional legal order', even before committing any criminal (let alone terrorist) offence. 'Targets' of this kind are increasingly selected through computer 'profiles.' Selection is based upon algorithms that are effectively unchallengeable, but inevitably generate large numbers of 'false positives' – innocent people being wrongly treated as suspected terrorists. Members of minority groups are more likely to be thus selected, leading to discrimination-by-computer. Yet by being presented as 'scientific' such discrimination is more difficult to challenge than previous, coarser stereotyping.

Even where 'data mining' and 'profiling' contributes to the apprehension of terrorists, there will always be a high proportion of 'false negatives' – real terrorists that are not identified as such. We are giving up freedom without gaining security. In the process, all of us are increasingly placed

under general, precautionary mass surveillance, with comprehensive data being captured on our activities.

The European surveillance society is developing in a profoundly undemocratic way. Massive data collection and trawling threaten the most fundamental values supposedly underpinning the European political settlement, at both national and international level. In its actions against terrorism, the EU Council in particular is doing the European ideal a serious disservice by undermining democracy and the rule of law on the Continent.

At a more practical level these issues will create serious problems for European and wider international co-operation in the fight against terrorism, including constitutional challenges to such arrangements in countries in which data protection is given a high level of protection under the national constitution. They will therefore ultimately undermine, rather than help, in the fight against terrorism.

References

Article 29 Working Party (2007). *Common Position of the European Data Protection Authorities on the use of the Concept of Availability in Law Enforcement*. (adopted 11 May 2007). URL (accessed 27 February 2008): http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_EU/07–05–11_Larnaca_availability_EN.pdf.

Bird, J. (2006). Terrorist Use of the Internet. The Second International Scientific Conference on Security and Countering Terrorism Issues, Moscow State University Institute for Information Security Issues, 25–28 October.

Brown, I. and Korff, D. (2004). *Striking the Right Balance: Respecting the Privacy of Individuals and Protecting the Public from Crime*. Wilmslow: Information Commissioner's Office.

Brown, I. (2007). The Law and Economics of Cybersecurity. *Law Quarterly Review 123*, 172–5.

Bowring, W. (2006). *The Human Rights Implications of International Listing Mechanisms for 'Terrorist' Organisations*. OSCE/ODIHR – UN HCHR Expert Workshop on Human Rights and International Co-operation in Counter-terrorism, ODIHR.GAL/14/07. URL (accessed 25 February 2008): http://www.statewatch.org/terrorlists/OSCE-UN-feb-2007.pdf

Carlile (Lord) of Berriew (2007). *The Definition of Terrorism*, Cm 7052. London: The Stationery Office.

Cobler, S. (1976). *Die Gefahr Geht von den Menschen aus: Der Vorverlegte Staatsschutz*. Berlin: Rotbuch.

Council of Europe (2002). *Guidelines on Human Rights and the Fight against Terrorism*. Strasbourg: Council of Europe Publishing.

Cownie, F., Bradney, A. and Burton, M. (2007). *English Legal System in Context*, 4th edn. Oxford: Oxford University Press.

Dutton, W. H. and Helsper, E. (2007). *Oxford Internet Survey 2007 Report: The Internet in Britain*. Oxford: Oxford Internet Institute.

European Commission (2005). *The Hague Programme: Ten Priorities for the Next Five Years. The Partnership for European Renewal in the field of Freedom, Security and Justice*. COM(2005) 184 final.

Ford, R. (2004). Beware Rise of Big Brother State, Warns Data Watchdog. *The Times*, 16 August. URL (accessed 28 February 2008): http://www.timesonline.co.uk/tol/news/uk/article470264.ece

Institute for Race Relations (2004). Arrests Under Anti-terrorist Legislation Since 11 September 2001. URL (accessed 27 February 2008): http://www.irr.org.uk/pdf/terror_arrests_study.pdf

Labi, N. (2006). Jihad 2.0. *Atlantic Monthly July/August*, 102–7.

Privacy International (2005). Discrimination and Anti-Terror Policy Across Europe. URL (accessed 27 February 2008): http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347–360509

Ryan, J. (2007). *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web*. Dublin: Institute of European Affairs.

Schjolberg, S. (2007). Terrorism in Cyberspace – Myth or Reality? URL (accessed 28 February 2008): http://www.cybercrimelaw.net/1–2007.html.

Schneier, B. (2006). Data Mining for Terrorists. *Schneier on Security*, 9 March 2006. URL (accessed 25 February 2008): http://www.schneier.com/blog/archives/2006/03/data_mining_for.html

Shahar, Y. (2007). The Internet as a Tool for Counter-terrorism. *Patrolling and Controlling Cyberspace*. NATO: Advanced Research Workshop, Garmisch-Partenkirchen, April.

Stenersen, A. (2007). Chem-bio Cyber-class – Assessing Jihadist Chemical and Biological Weapons. *Jane's Intelligence Review 1 September*, 8–13.

US Army (2005). *Army Regulation 530–1, Operations Security (OPSEC)*. 19 April 2007.

US National Research Council (2008). *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*. Washington, DC: National Academies Press.

Vervaele, J. (2005). Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law? *Utrecht Law Review 1*(1), 1–27.

Walker, C. and Akdeniz, Y. (2003). Anti-terrorism Laws and Data Retention: War Is Over? *Northern Ireland Legal Quarterly 54*(2), 159–82.

Ian Brown

Ian Brown, PhD, is a research fellow at the Oxford Internet Institute, where he studies public policy issues around information and the Internet, particularly privacy, copyright and e-democracy. He also works in the more technical fields of information security, networked systems and healthcare informatics. During 2009 he is undertaking a study for the European Commission on future data protection law.
ian.brown@oii.ox.ac.uk

Douwe Korff

Douwe Korff is Professor of International Law at London Metropolitan University, specializing in human rights and data protection. He has recently carried out research and provided training for judges, procurators, advocates and human rights activists across central Asia. He was counsel for the applicant at Strasbourg in cases including *McCann* v *UK* (the 'Gibraltar Shooting Case') and *Castells* v *Spain* (on freedom of expression).
douwe.korff@londonmet.ac.uk