18th BILETA Conference:*Controlling Information in the Online Environment*

April, 2003
QMW, London

Privacy, data retention and terrorism

Diane Rowland
University of Wales, Aberystwyth

Introduction

To what extent is the protection of individual privacy outweighed by the collective requirements of a safe society particularly in the light of the avowed war against terrorism? Governments seem to have become increasingly concerned as to whether they do, indeed, possess sufficient powers to track not only terrorist but other criminal activity and one particular concern has been the ease with which communication takes place via global communication networks such as the internet creating a perceived need to track such communications. Accordingly, there have recently been considerable legal and political developments on for instance, exchange of personal data, data retention and surveillance which could have adverse consequences for the rights of the innocent internet user. These initiatives have been given a further impetus by the events of 11 September 2001, the inception of the 'war' against terrorism and more recently the war in Iraq, although in many cases their origins can be traced back further than this. Since September 11th, a wide range of governments have introduced legislation which allows generalised retention of computer traffic data and other personal details of those who communicate via the internet. Thus it was reported that the EU's Justice and Home Affairs Minister decided in the aftermath of Sept. 11th that law enforcement agencies need access to all traffic data for the purpose of criminal investigations in general and not limited to terrorist activity[1]. A significant number of 'Western democracies' including the US and member states of the EU have enacted or amended legislation, as well as jurisdictions which are more readily recognised as being repressive about their citizens' use of the Internet. This paper will examine the recent legal and political developments in these areas and analyse and assess the balance between the requirements of law enforcement agencies, state security, ISPs and the rights of the individual.

Data retention and data protection in the European Union

There are schools of thought suggesting that data protection law is an outdated and cumbersome approach to the protection of privacy on-line particularly in its application to global networks. Nevertheless, it is still the case that in the European Union, general rules dealing with the retention of personal data are covered by Article 6(1)(e) of Directive 95/46/EC[2] which requires that personal data should be kept in a form which permits identification of the data subject for no longer than necessary for the purposes for which the data were collected. The provisions of article 6 are subject to the general exceptions including national security, defence etc in Article 13. These rules were intended to provide a sufficient balance between the requirements of individual privacy and the needs of law enforcement and state security. The UK Information Tribunal (National Security Appeals) in a case involving the MP, Norman Baker[3], emphasised the need to apply strict criteria of proportionality in cases of derogations from the rights provided to data subjects, particularly in

relation to national defence and security. Thus in the absence of specific exceptions, personal details relating to all computer traffic data should be erased or anonymised and the only legitimate purpose for retaining any such data is for billing purposes. Amplification of the data protection rules for the communications sector was later accomplished in Directive 97/66/EC[4] which referred to the increasing risk connected with automated storage and processing of communications networks and the need for users to be assured that privacy and confidentiality would not be compromised. This directive has now been repealed and replaced by Directive 2002/58/EC on privacy and electronic communications [5]. This directive makes provision for a number of perceived problems e.g. Spam and cookies for instance, but also makes some potentially far-reaching changes relating to data retention. Article 15 of this Directive now allows Member States to adopt legislative measures for the retention of data for a limited period if necessary to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences etc., although any such measures are required to comply with the general doctrines of EC law such as proportionality and respect for human rights. If article 15 is not invoked then the rules require mandatory destruction of data by virtue of article 6. It appears that the implicit inference from Article 15, together with the fact that all of these directives are not intended to apply to those areas of law not within Community competence, is that matters of security and law enforcement are likely always to take precedence over matters of individual privacy but that this should be neither an automatic presumption nor an inevitable outcome. The new provision is widely drafted and potentially makes little distinction between the action which may be taken in response to extreme terrorist activity and more routine criminal behaviour. This makes its difficult to apply the doctrine of proportionality which is at the heart of EC law and which requires a balance of risks and consequences. Further, ISPs will bear a significant burden as a result of the new rules in terms of responsibility for the tracking and retention of the relevant data. A joint statement of the European Internet Services Providers Association (EuroISPA) and its US counterpart (US ISPA) on 30 September 2002[6] expressed the view that 'Governments have not sufficiently demonstrated that the absence of mandatory data retention is detrimental to the public interest', that mandatory data retention in the absence of any business purpose would 'impose serious technical legal and financial burdens on ISPs' and that 'privacy, due process, transparent procedures and fair and equal access ... should not be jeopardized unless there is a compelling and lawful need.' They call for the replacement of data retention laws with data preservation which based on the G-8 definition does not include prospective collection of data and neither does it require ISPs to collect and retain data not required for ordinary business purposes. This burden on ISPs is perhaps not easily reconciled with the policy reasons behind the increasing provision of immunity suit with which they are being endowed in other areas.

Opponents of this view will argue first that the rules are concerned with the retention of data and not content but in the context of the internet, traffic data can include e.g. a list of URLs visited which can easily be correlated with actual content. Another opposing argument is that such an outcome is not inevitable as the wording of Article 15 is permissive not mandatory but independently a number of Member States, including the UK, have in any case already made provisions for data retention and there is apparently now in existence a draft Framework Decision on the retention of traffic data and access for law enforcement agencies[7]. The purpose of this draft decision is to 'make compulsory and harmonise the a priori retention of traffic data in order to enable subsequent access to it, if required, by the competent authorities in the context of a criminal investigation.' The preamble makes reference to the right to privacy but asserts that 'a period of a minimum of 12 months and a maximum of 24 months for the a priori retention of traffic data is not disproportionate in view of the needs of criminal prosecutions as against the intrusion into privacy that such a retention would entail.' However there are no details of how these figures are arrived at, what manner of risk assessment has been carried out etc. The draft decision further defines the categories of data which can be retained namely that necessary to:

- follow and identify the source of a communication
- identify the destination of a communication
- identify the time of a communication

- identify the subscriber
- identify the communication device

These measures taken together would create some fairly drastic changes in the approach to the protection of privacy on-line but have not been accepted with approval in all quarters. The issues were aired in March 2003 when the Committee of Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament held a public seminar entitled 'Data Protection since 11 September 2001: What strategy for Europe?' Topics for consideration were the need to strike the appropriate balance between the requirements of freedom and security in the light of 'undifferentiated access to data of all kinds in order to detect threats of terrorism and organised crime at the earliest possible stage.'[8]

The Article 29 Data Protection Working Party in its Opinion[9] on the need for a balanced approach in the fight against terrorism called for the 'need to establish a comprehensive debate on the initiative to fight terrorism and the fight against criminality in general, as well as limiting the procedural measures which are invasive to privacy to those really necessary.' It was particularly concerned about the long term impact of what could be described as knee-jerk policies and reactions especially in the light of the fact that 'terrorism is not a new phenomenon and cannot be qualified as a temporary phenomenon.' It called for any legislation which limited the right of privacy to be sufficiently clear in 'its definitions of the circumstances, the scope and modalities of the exercise of interference measures' many of which as we have already seen are potentially very wide and even uncertain in scope. Finally it concluded that 'measures against terrorism should and need not reduce standards of protection of fundamental rights which characterise democratic societies. A key element of the fight against terrorism involves ensuring that we preserve the fundamental values which are the basis of our democratic societies and the very values that those advocating the use of violence seek to destroy.' These concerns are echoed in a statement from the European Data Protection Commissioners noting with concern the proposals for systematic retention of traffic data and expressing 'grave doubt as to the legitimacy and legality of such broad measures' and going as far as to say that 'systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case.'[10]

In the UK, the Anti-terrorism, Crime and Security Act 2001 contains provisions which allow communications service providers to retain data about their customers' communications for national security purposes. It allows for setting of codes of practice in consultation with the Information Commissioner but also gives the Secretary of State powers, in ss104(1) and (2), to make orders connected with the retention of communications data directed to communications providers generally, specifically or particularly.[11] The current proposal is that this will be accomplished by means of a voluntary code for ISPs. The Information Commissioner remains 'unconvinced that there is a need for communications service provider to retain data routinely for the prevention of terrorism for any longer than data would normally be retained for business purposes' but that if such a need is proven there is no justification for making the code voluntary. Despite these reservations, the draft Code of Practice on Data Retention issued by the Home Office for consultation in March 2003[12] is usually described as being drafted in consultation with the Information Commissioner.

The situation in the US

Whereas in the context of the internet, Europe seems to be focusing on data retention, there appear to be no plans for such provisions in the US. However far from this indicating US opposition to such rules, it could be argued that, in the absence of generic data protection legislation, such rules are not essential in the US in order to achieve data retention. The official US stance is certainly against mandatory destruction rules on the basis that 'traffic data and mobile device location data are critical to apprehend terrorists and criminals and to prevent the execution of planned terrorist and criminal acts'[13]. Post-September 11th, the US has enacted the US PATRIOT Act 2001[14] and the Homeland Security Act 2002 which, in this context, increase dramatically the available powers of

electronic surveillance and interception. They are couched in similarly broad terms and are equally capable of unacceptable intrusion on the on-line privacy for the innocent. They allow law enforcement agencies to trace and record computer routing addressing and signalling information and to gain access to e.g. personal financial information purely on the basis that the information is likely to be relevant to an investigation. The effects of this statute have been described as 'both the diminishment of personal privacy and the expansion of government secrecy.'[15] The most recent proposals concern the draft Bill of the Domestic Security Enhancement Act of 2003[16] (being referred to as PATRIOT II) which will, inter alia, criminalise the use of encryption.

Conceptually the approaches of Europe and the US are remarkably close to each other and notwithstanding previous debates on data protection issues as epitomised in the Safe Harbor negotiations, there is evidence that in areas of state security and criminal law enforcement there is a much greater degree of consensus. This is shown also in the US participation in the Cybercrime Convention[17], although this makes provision for data preservation in specified situations rather than blanket retention as detailed in article 16(1):

> Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. At the time of writing there are also apparent proposals for an exchange of personal data between Europol and the US which would raise similar concerns[18].

Conclusion

Both security and privacy are important and fundamental concepts both for individuals and collectively for society but neither are amenable to quantification. The practical problem is how to achieve a proportionate response which responds to the threat or perceived threat from terrorism and other criminal activities. How should the risk from terrorism or lesser criminal activity be assessed? Whilst not wishing to dispute the need for a global approach to international terrorism the current developments do not seem to provide a proportional response to the threat and that the same end could be achieved by measures which have a lesser impact on the ordinary internet user.

The first question which could be addressed is whether existing data protection law really does provide a safe haven for terrorists. Would a rigorous application of the existing law be capable of addressing the current concerns? Data protection law already contains sufficient exemptions which appropriately applied would cover the requisite subject matter. If the purpose of processing is a legitimate one then the data can be retained as long as is necessary without breaching existing data protection principles. Recent events have certainly enhanced the public's apprehension and fear of terrorist and other criminal activity even if these fears are, if not entirely groundless, based on an exaggerated assessment of the likelihood of adverse consequences. One of the most intractable problems is the difficulty in dealing with both the public's and the politicians' perceptions of the risk posed by terrorism and almost tacit acceptance of the need to take measures which in different circumstances would be rapidly identified as draconian and disproportionate. Justice William Brunna (dissenting) in *Brown v Glines*,[19], albeit in a different context, expressed similar reservations thus:

> '... the concept of military necessity is seductively broad and has a dangerous plasticity. Because they invariably have the visage of overriding importance there is always a temptation to invoke security 'necessities' to justify an encroachment on civil liberties. For that reason the military security argument must be approached with a healthy scepticism ... its very gravity counsels that courts be cautious when military necessity is invoked by the Government to justify [an infringement of civil liberties]'.

Nevertheless this is certainly not to say that society's perception of risk should be ignored. Real perceptions of risk contribute significantly to what the public expects from its politicians and regulators even if these perceptions are based on false or over-stated premises.

If, taking all these factors into account, the assessment is that existing data protection law is inadequate to deal with the threat (bearing in mind that, notwithstanding the severity of recent terrorist attacks, it is not clear that the probability of such attacks is actually increasing) then the proportionate response is surely to create a measured statutory response, not dependent on voluntary compliance and codes, but which is carefully and narrowly constructed and contains appropriate safeguards subject to proportionality. Thought could be given to the use of data preservation rather than data retention and relevant safeguards could include assurances that any data provided were to be used in an investigation and were not collected 'just in case'. This would still leave some not inconsiderable residual questions to be addressed concerning compliance with other data protection principles such as subject access, security etc.

---

[1] See e.g. www.statewatch.org/mews/2002/aug/05datafd1.htm, before September 11th the President's Working Party on Unlawful conduct on the Internet (March 2000) had concluded that law enforcement needs and challenges posed by the Internet were significant and called for new investigative tools and capabilities.
[2] In the UK this is implemented in the Data Protection Act 1998 Schedule 1 Principle 5 (i.e. the 5th Data Protection Principle).
[3] *Norman Baker MP v Secretary of State for the Home Department* Information Tribunal (National Security Appeals) 1 October 2001 available from www.lcd.gov.uk/foi/bakerfin.pdf.
[4] [1998] OJ L24/1.
[5] [2002] OJ L201/37 to be implemented by Member States by October 2003.
[6] See www.euroispa.org.
[7] See www.statewatch.org/news/2002/aug/05datafd1.htm.
[8] See e.g. outline programme at www.statewatch.org/news/2003/mar/hearing-25-03.htm.
[9] Opinion 10/2001 adopted on 14 December 2001 (0901/02/EN/Final) see http://europa.eu.int/comm/internal_market/workinggroup/wp2001/wpdocs01.htm.
[10] See www.fipr.org/press/020911DataCommissioners.html and see also Opinion 5/2002 of the Article 29 Working Party on Data Protection, http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2002/wpdocs02.htm.
[11] Anti-terrorism, Crime and Security Act 2001 s 104 (1) and (2).
[12] www.homeoffice.gov.uk/docs/vol_retention.pdf.
[13] See e.g. Mark Richards representing US Government at European Union Forum on Cybercrime, Brussels November 2001.
[14] Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism Act.
[15] Marc Rotenberg 'Privacy and Secrecy after September 11' (2002) 86 Minn L Rev 1115.
[16] See e.g. www.aclu.org/SafeandFree/ and David Cole 'What PATRIOT II Proposes to do' www.cdt.org/security/usapatriot/030210cole.pdf
[17] Article 16 Convention 185 on Cybercrime http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
[18] See www.statewatch.org/news/2002/nov/12eurousagmt.htm.

[19] 444 US 348, 62 L Ed 2d 540, 614 (1980).