Parliamentary Office of Science and Technology

postnote

October 2002 Number 183

ELECTRONIC PRIVACY

The growth in use of the internet and other forms of electronic communication has resulted in a significant increase in the capacity to collect and process data about individuals electronically, with consequent implications for personal privacy. Concerns have also been expressed about the privacy aspects of recent legislation aimed at curbing terrorism and crime. This note examines the potential for commercial organisations and the public sector to infringe the privacy of digital communications, how the law can protect such communications and the implications for Government policy.

Background

Public concern about privacy is rising. Figures from the Office of the Information Commissioner[1] show an almost threefold increase in enquiries about data protection over the past two years. Two main areas contribute to these concerns, both governed by existing legislation:

- the data gathering and processing practices of commercial organisations, and
- the Government's power to access personal communications.

There is a danger that failure to address the public's privacy fears could dampen the success of electronic services such as new mobile phones and internet shopping, as well as affecting the Government's aim of making all its services available electronically by 2005.

Privacy from commercial organisations

Electronic communications now form an essential part of our society, be it through credit card purchasing, on-line shopping or communication by mobile phone. The ease with which details of these communications can be recorded allows collection of data at an unprecedented level of detail. Coupled with increasing computing power allowing more effective analysis and processing of this data, this enables electronic service providers to build up detailed pictures of their customers' activities. Some examples of how this can be achieved are given in the box opposite.

Collecting and using consumer data

The internet

Many websites request personal data such as name, address and email address from visitors. In addition files known as 'cookies' or 'webbugs' or so-called 'spyware' programs can be used to monitor a user's on-line activity, often without the user's knowledge. This enables an extensive picture of the user's on-line activity to be developed including, for example, details of websites visited or online purchases, or the user's email address. Although the data collected is originally correlated to a particular computer rather than an identifiable individual, its quantity and nature could in some cases allow "off-line" identities to be deduced.

Digital TV sets

Digital video recorders and the "set-top boxes" used to receive digital TV can communicate with the provider company to report customer viewing habits or send messages to the viewer. The BBC was recently criticised by consumer and privacy groups for downloading a new sitcom to TiVo digital video sets without their owners' permission.

Telecommunications service providers

Telecommunications companies are entitled to keep records of their customers' activities for a limited time for billing purposes or, with the customer's consent, for marketing purposes. Such records could include numbers called or websites accessed, length or time of call, and caller location.

Store cards or credit cards

Store cards or credit cards can gather information on individual transactions carried out by consumers using these cards. The volume of data gathered means it is rare for this to be analysed at individual customer level. Instead it is used to group customers for targeted marketing purposes.

Collection of consumer data can enable personalisation of electronic services, for example to allow more efficient service delivery or individually targeted advertising. This ability to tailor services to individual consumers continues to be an important driver in the development of electronic services and in particular in the development of the internet, on which many sites are provided free to the user. Many privacy advocates accept that the use of

targeted advertising as a means of funding electronic services is an acceptable business model. Nonetheless, the manner of data collection and degree of consumer consent to the uses made of the data have raised concerns, discussed in the issues section of this note.

Privacy from Government

Electronic communications raise new challenges for governments in balancing the right to individual privacy with the need to protect the public. The controversial Regulation of Investigatory Powers Act 2000 (the RIP Act) and the Anti-Terrorism, Crime and Security Act 2001 provide public authorities with new powers to fight terrorism and crime, including powers to intercept and access details of electronic communications and to demand plain text of encrypted messages.

Legislative framework

Data protection law

Protection for personal privacy in the UK currently derives largely from the Data Protection Act 1998 (see box below), itself derived from the 1995 EU Data Protection directive. Responsibility for enforcement of the Act falls to the Information Commissioner. As well as investigating reports of non-compliance, the Information Commissioner works with businesses to ensure their practices comply with the law.

Data Protection legislation

The Data Protection Act 1998

The Act requires anyone processing, obtaining or disclosing personal data to comply with the eight data protection principles. The data must be fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate; not kept longer than necessary; processed in accordance with the data subject's rights; secure; and not transferred to countries without adequate protection. Exemption from the Act is given where compliance could prejudice national security or crime prevention and detection.

The new Privacy and Electronic Communications Directive

The directive requires EU member states to strengthen data protection measures in a number of areas:

- '**spam**' – Prior permission from the recipient ('opt-in') is required before sending unsolicited messages, whether by email, SMS (text message) or fax (although 'opt-out' can apply for existing customers).
- **cookies** – Websites must inform users what any downloaded files (such as cookies) are for, and allow customers to refuse them.
- **directories** – Subscribers must have a choice as to whether their personal data is published in any listing of subscribers to a particular service, such as a telephone directory.
- **location data** – This must be processed only with the consent of the user.

The EU Data Protection Directive is supplemented by a specific directive for the telecommunications sector, which has recently been reviewed in the light of the proliferation of new electronic communications services. The revised Directive on Privacy and Electronic Communications[2] is due to be incorporated in UK law by end October 2003, following a consultation due to take place from January to April 2003. The Directive increases consumers' control over how their personal data is processed in the electronic world, but has been criticised for allowing communications providers to retain traffic records in certain circumstances (see box).

Access to communications

The RIP Act permits the Secretary of State to issue a warrant for interception of communications where this is necessary for national security or for detection or prevention of serious crime[3]. Use of this power and the RIP Act powers described below is overseen by the Interception of Communications Commissioner, while complaints about the use of the powers in the Act are heard by a tribunal established under the Act.

The RIP Act and several other recent legislative initiatives contain measures relating to traffic data i.e. data associated with a communication other than its content, such as date and time of the communication, number called or website visited, or location of the caller. These are described in the box below.

Legislation on access to or retention of traffic data

- The **Anti-terrorism, Crime and Security Act 2001** (the ATCS Act) allows a voluntary code of practice to be drawn up allowing retention of traffic data by communications providers for national security reasons.
- The **RIP Act** permits designated officers in law enforcement agencies to demand disclosure of traffic data for a range of purposes, including preventing and detecting crime, public safety, public health and tax collection.
- The new EU **Directive on Privacy and Electronic Communications** allows member states to require communications providers to retain traffic data in the interests of national security or crime prevention.
- The **EU Council** is currently considering separate proposals to harmonise traffic data retention provisions across the EU.
- **Sector-specific legislation** permits certain public authorities to request access to traffic data. In some cases data disclosure is discretionary, leaving communications providers to judge whether a particular access request is legal.

Issues

Does data protection law work?

Most of the data gathering activities carried out by commercial organisations and described in the box on page 1 are subject to data protection law. Nevertheless, it is unclear whether there is full compliance with the law across the electronic sector.

Subscriber data

Data collected by providers of electronic services, such as websites, digital TV or mobile phone companies, may be stored by reference to the relevant computer address or subscriber number rather than to a named individual. It is not clear whether such data constitutes 'personal data' and hence whether it falls under the Data Protection Act. Arguably such data should be clearly protected regardless of whether the individual concerned is identified by name.

Enforcement
The Information Commissioner has expressed concern about the protracted nature of current data protection enforcement procedures[1]. These are particularly ill-suited to the electronic environment, where a non-compliant website or service could relaunch under a new name before any lengthy enforcement proceedings were completed. Introduction of regulations to implement the privacy and electronic communications directive may provide an opportunity to address this issue. Discussions are underway between the Information Commissioner and the DTI to this end.

The internet
A study by consumer watchdog Consumer's International on privacy on the internet[4] found that the data collection practices of many EU-based websites did not comply with EU law. Customers were rarely provided with a choice as to whether their name was added to a mailing list or whether their data was shared with other parties. By contrast US-based sites were more likely to comply with EU data collection practices, despite the lack of privacy legislation in the US. The study ascribed this finding to pressure from privacy-conscious US consumers, suggesting that legislation may be most effective when combined with consumer pressure.

Consumer awareness
The Information Commissioner's enforcement of data protection law consists largely of reacting to complaints of non-compliance rather than proactively checking that organisations comply with the law. The effectiveness of enforcement is therefore crucially dependent on consumer awareness of the law. Similarly, although the new EU directive on privacy and electronic communications has the potential to increase personal privacy in electronic media, the effectiveness of its implementation may depend considerably on consumer awareness of its provisions. Moreover, many electronic services accessed by UK consumers are provided from overseas countries with less strict privacy laws than the EU. Here privacy will again depend on consumer awareness. However, the Information Commissioner reports that only 42% of the public are aware of their rights under Data Protection law[1] (although this figure as risen from the 20% level typical over the past decade). On the other hand, some commentators argue that this figure, and the public's continuing willingness to release personal data, simply reflect the fact that privacy is not a major concern for many members of the public.

A number of industry-led initiatives exist which aim to protect consumer privacy on the internet (see box opposite). Although such initiatives could potentially reduce the need for consumer awareness, some privacy watchdogs have argued that these initiatives may infringe rather than protect consumer privacy.

Alternatively, individuals can take steps to enhance their privacy. Pre-pay mobile phones can be purchased without providing any ID. Commercially available privacy enhancing software can strip internet traffic of identifying features, allowing anonymous and untraceable use of email and the web; control the circumstances in which a computer will accept cookies or unsolicited emails; or encrypt communications. However, such services may be within the reach of technologically literate consumers only, and security services have expressed concerns that they could aid criminal activity.

Industry led on-line privacy initiatives

- Users registered with **Microsoft Passport** provide personal details which can be automatically shared with Microsoft Partner sites to which they login. Partner sites must display privacy statements explaining how personal data will be obtained and used. Critics argue that rather than protecting privacy, this system in fact facilitates exchange of personal data and provides a single company with too much control over individuals' personal information.
- The 2180 members sites of the UK-based **Which? Web Trader** scheme must adhere to certain privacy and security standards. Compliance with these standards is verified by the Consumer's Association.
- The Worldwide Web Consortium's **Platform for Privacy Preferences** project (P3P) establishes common standards for recording website privacy policies. By presenting these policies in a user-friendly format it enables informed choice by the user as to whether to release personal information to a particular site. The latest versions of the most common internet browsers are P3P-enabled and around a quarter of the US's most popular internet sites are P3P compatible. Many user groups and commentators have welcomed the system as empowering the user to control their information. But some critics argue that it absolves companies of responsibility for their use of that information, and point out that there is no system to verify that websites adhere to their declared privacy policy.

Effect on e-commerce
Some have argued that the new EU directive on privacy and electronic communications could impact on the development of electronic commerce. The directive prohibits sending unsolicited electronic communications such as email and SMS messages unless the customer has previously 'opted in' to receive them. The Direct Marketing Association is concerned that this could penalise small companies which rely heavily on direct marketing, while providing little protection for consumers from 'spam' email, much of which originates outside the EU. They would have preferred to continue with the 'opt-out' approach used for unsolicited phone messages.

Privacy from Government
Industry and privacy groups have expressed a number of major concerns relating to implementation of both the RIP Act and the Anti-terrorism, Crime and Security Act (the ATCS Act). Many of these issues were highlighted by the Government's recent proposal to extend the list of public authorities which could demand access to traffic data under the RIP Act to include local authorities, some Government departments and bodies such as the Environment Agency and Postal Services Commission. The considerable protests which greeted this proposal led to its withdrawal pending further consultation in autumn

2002; a number of the issues below will be relevant to and addressed in that consultation.

Targeting
It may not always be possible to intercept exclusively those communications relevant to a particular investigation (for example, it is not possible to intercept exclusively phone calls made by one individual on a shared landline). In the case of warrants permitting interception of communications of a type specified in the warrant this 'collateral intrusion' may be acute. Privacy groups fear that such warrants could be used to trawl all communications for chosen keywords. While a warrant may only be issued if the Secretary of State believes the impact of any collateral intrusion to be proportionate in comparison with the need for the warrant, some privacy groups remain concerned that independent oversight of the Secretary of State's judgement is confined to retrospective review of the decision-making process.

Legal concerns
While the ATCS Act allows retention of traffic data only in the interests of national security, the RIP Act allows access to any data retained for a number of reasons, of which national security is only one. The Information Commissioner has expressed "real concern" that this could allow data retained for national security purposes to be accessed for a variety of unrelated other purposes, and that this could be "arguably unlawful" under the privacy provisions of the European Convention on Human Rights (ECHR). The Home Office maintains that once stored, data can be accessed lawfully for any of the purposes in the RIP Act, and intends to continue with implementation of both acts. This legal question may remain unresolved without a court judgement. European Data Protection Commissioners have also expressed doubts as to the legality of data retention provisions currently under consideration in the EU Council, again due to concerns about compatibility with the ECHR.

Authorisation requirements
The RIP Act authorises officers in law enforcement agencies, of a rank specified by order, to access traffic data. There is concern that numerous officials with little experience or training in judging a request's technical feasibility, or whether its privacy impact is justified, could be authorised to access traffic data. Extension of the act to allow more public bodies to access traffic data could increase the potential for abuse of this power. Privacy advocates are also concerned that such an extension could empower public bodies to access traffic data for any of the purposes listed in the RIP Act, regardless of whether these were relevant to the authority's functions (although in practice it would be difficult for the authority to justify as necessary or proportionate access for purposes unrelated to their functions).

The Home Office argues that bringing public authorities within the RIP Act framework would in fact increase scrutiny and oversight of traffic data requests, for example by requiring the rank of official who may request traffic data to be specified by order. They also point out that only those public bodies who already make access requests under other legislation were included in the proposed extension of the act.

Storage and retrieval
Under the ATCS Act, companies will be required to retain data for lengths of time specified by Government. Any requirement on a company to retain traffic data for considerably longer than they currently do for business purposes could be technically and financially burdensome. For example, the company storage system is unlikely to be designed to cope with the quantity or level of data accuracy requested by Government.

If the quantity of traffic data stored grows, retrieval of data in a cost effective and timely manner is likely to become increasingly difficult. Communications providers are concerned that satisfying requests from individuals to see data stored about them is likely to cost considerably more than the £10 maximum which they are permitted to charge under the Data Protection Act.

Oversight
Both the Interception Commissioner and the Parliamentary Intelligence and Security Committee have expressed concerns over the ability of the Interception Commissioner and Tribunal to cope with the additional workload arising from implementation of the RIP Act powers on access to traffic data. While the Government has committed to provide the Commissioner with the resources required, any extension of the RIP Act powers could highlight this issue. It could also prompt consideration of whether the Tribunal's current secretive working methods were appropriate to appeals about activity unrelated to national security or serious crime.

Overview

- Legislation alone is not sufficient to protect privacy; consumer education also plays an important role
- Rigorous implementation of safeguards could go some way towards allaying privacy fears relating to Government powers to access communications.

Endnotes

1 Information Commissioner, *Annual report and accounts for the year ending 31 March 2002*, HC913.
2 Directive 2002/58EC on the processing of personal data and the protection of privacy in the electronic communications sector.
3 Interception may also be authorised in the interest of safeguarding the economic well-being of the UK, where this is directly related to national security.
4 Consumer's International, *Privacy@net: An international comparative study of electronic commerce and data protection,* January 2001.

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of public policy issues that have a basis in science and technology.

The Parliamentary Office of Science and Technology, 7 Millbank, London SW1P 3JA Tel 020 7219 2840

www.parliament.uk/post/home.htm