

Risks of sharing customer data with government authorities

By Eugene Oscapella

ENLISTING THE HELP OF BUSINESSES for government surveillance – is it a case of little brother joining big brother? *PL&B International* looks at governments' efforts to gain access to the private sector's databases.

Relying on businesses to provide information to government investigators has a long history. In some countries, companies have willingly provided personal data about clients to government investigators, even if not legally required to do so. Others challenge their governments to prove the legal authority to obtain access to the data. Still other companies, discreetly and for profit, yield the personal data they hold. For example, in April 2001, the *New York Times* reported an alleged arrangement between US railway company, Amtrak, and the Drug Enforcement Administration to help identify drug couriers in exchange for a percentage of the seized assets (*PL&B Int*, May 2001, p.27).

Concerns about national security have added fresh impetus to the search for useful information, whether held within or outside government. A recent report funded by US task force, the Markle Foundation, and entitled *Protecting America's freedom in the information age*, examines the challenges of sharing information in the name of protecting national security. The report calls for a networked information technology system that effectively shares information among local, state, regional and federal agencies, and the private sector.

One background study published with the report examines the possible use of personal information held by the private sector in preventing terrorism.

The study examines the various legal processes now available to the US government to obtain access to personal information held by third parties, includ-

ing search warrants and subpoenas. It describes the rules applicable to specific types of information: information about communications, financial records, cable (television) viewing records, video rental records, and educational records. As such, the report is a useful summary for businesses of the multiplicity of American laws on government access to data held by the private sector.

The study also identifies possible problems with traditional means of obtaining access to data held by private sector bodies: "Using data mining techniques to isolate suspicious behaviour in masses of privately-held data – data about mostly innocent people – does not fit the typical 'search' model. Instead, the government will usually have to process the data for suspicious patterns before it will even know whether further investigation is warranted. Allowing such processing may well be important to the anti-terror campaign. It also raises privacy issues that cannot be ignored."

The study notes two concerns beyond the threat to civil liberties posed by such business-government data sharing – private sector fears about liability for disclosure, and the cost of disclosure: "In addition to the restrictions that the government faces in accessing information held by private parties, the parties themselves also have legal concerns about sharing the information with the government. The two principal concerns that private entities have when complying with government requests are: liability and reimbursement."

As the study notes, the risk of lia-

bility arises not just through US law. In many ways, it says, foreign laws present a greater obstacle to sharing information. Many companies from which the government might request information – such as financial institutions, airlines and telecommunications companies – are multinational corporations subject to foreign privacy laws, including the EU Data Protection Directive and other data protection laws. Cautions the study, "practically all databases outside the United States are subject to some data protection restrictions – enforceable through fines, jail terms and private lawsuits."

The study does not address (and perhaps it should not, since it is primarily a legal analysis) the likely increase in consumers' reluctance to share information with businesses that have a closer relationship with government authorities. Yet this is clearly a significant issue for business around the globe as they seek to gain or maintain the trust of consumers.



A report is available from Stewart A Baker, "The regulation of disclosure of information held by private parties", in "Protecting America's freedom in the information age: A report of the Markle Foundation Task Force", October 2002: www.markletaskforce.org