Terrorism, Business and Data Protection

Report by Eugene Oscapella

MUCH HAS ALREADY BEEN WRITTEN about the broad impact on privacy of the hurriedly cobbled-together anti-terrorism laws of many Western countries. There is little point in adding to the general debate. However, we might consider the direct impact of these laws and of evolving attitudes to privacy on the personal data handling practices of businesses.

These new laws will undoubtedly place organisations under greater pressure to collect and share personal data with governments. However, even without any added legislative authority, government agencies may simply try to persuade, or even deceive, organizations into disclosing personal data. A recent report in the *Washington Post* suggested that such "informal" requests are already on the increase in the US: a former federal prosecutor who specializes in government investigation work reported visits to several of his clients by federal agents since 11th September.

Organizations holding personal data must inform themselves about the potential legal consequence of disclosures other than those permitted or required by law. Even well-intentioned cooperation by an organization with a government agency for a laudable purpose might land organisations in hot water for violating data protection laws.

Economic intelligence may become less of a priority, unless that intelligence is directly related to a terrorist threat. The US-based Cato Institute, a libertarian think tank, pleaded for the United States to move away from economic espionage in a 1996 research paper (www.cato.org/pubs/pas/pa-265.html). The paper argued that America's intelligence agencies should devote their resources to the most serious security threats, principally international terrorism and adverse political trends. "Instead, the Clinton administration has diverted the intelligence community to economic espionage." Furthermore, the paper argued that economic espionage damages relations with governments whose cooperation the US may need in dealing with significant security threats: "Indeed, Washington's use of the Central Intelligence Agency for economic spying has already led to ugly incidents with Japan and France."

Not only Japan and France are upset. Strong hints of the EU's dissatisfaction with economic espionage can be seen in the 5th September 2001 vote of the European Parliament about the ECHELON intelligence system. [PL&B September '01, p.4] The European Parliament voted to accept a report that criticised intelligence services that allow themselves to be used to gather competitive intelligence. Both the United States and United Kingdom were singled out for their alleged roles in collecting economic intelligence.

While economic intelligence gathering comes under criticism on the one hand, pressures are mounting for increased monitoring of financial flows. And governments anxious to leave no stone unturned may err on the side of excess, supporting the massive gathering of economic intelligence, including personal data held by organisations. Thus some aspects of economic intelligence may become much less important, while others may gain new prominence.

Secure encryption, at least, secure from government, may well become a thing of the past. The pressure that arose in the US during the last decade to provide "back doors" to allow governments to decipher the encryption is increasing. Using encryption that cannot be deciphered by government may become an offence. Thus businesses may soon be able to use encryption to protect their corporate secrets from other businesses, but not from governments.

And where even expanded powers of search and seizure prove inadequate to slake the thirst of governments for personal information, will those same governments try to conscript or encourage businesses, which may not be subject to the same legislative restrictions as governments, to act in the stead of governments? Readers will recall [PL&B, May '01, p 27] that US railway company Amtrak was "sharing" information about passen

continued on page 6