Privacy vs public safety

Report by Merrill Dresner

DIMINISHING PRIVACY TO ENHANCE public safety does not justify business misuse of personal information. Last month's *Scientific American* conference looked at how the balance between liberty and national security is being managed outside the USA.

In partnership with the Centre for Strategic Studies (CSIS), *Scientific American* held a conference in New York in early March, entitled *Preserving an Open Society in the Age of Terrorism.* Originally scheduled for last autumn, to examine the privacy issues important for multinational companies, the focus of the conference suddenly changed in urgency and dimension in the aftermath of the September 11th attacks. The restructured conference brought together global experts from government, technology, law, healthcare, finance, privacy and security, and focused on defining a new security framework in the war against terrorists. How will the US manage the balance between personal liberties and public safety and what are the new reponsibilities for business? These were some of the questions posed.

OPPOSITION TO GOVERNMENT ACTION

Many experts expressed disquiet at the US government's eagerness to access business data to add to their arsenal of anti-terrorist weapons. There were warnings about increasing government oversight, pointing out that areas such as money laundering already have strong regulation to help security and intelligence. Strong opposition was expressed to giving the government any new powers in certain privacy arenas – key escrow (strong encryption) is the most prominent example of this debate. The conference tackled nuclear threats, bio-terrorism, authentication, verification and medical privacy. Day two was entitled *Homeland Security in Government and Business* – a title for a US conference which a year ago would have seemed unimaginable.

MEASURED APPROACHES TO LEGISLATION REQUIRED

The fundamental question asked, was whether privacy and security are necessarily at the opposite ends of a spectrum. Can there be a clear distinction between privacy of personal information and privacy of businesses and their transactions? Australia's Privacy Commissioner, Malcolm Crompton, in a session on *New Ground Rules for a Post 9/11 World,* was one of the voices urging a cautious and measured legislative response. He offered the following ideas as a starting point for debate on new security measures:

1. establish the scale of the problem.

2. determine whose privacy will be affected, taking into account whether the measures are likely to confront people's expectations about their right to privacy.

3. ask whether or not the measures will work. Do they emerge from thorough analysis and debate, and do they have community support?

4. ensure the measures are proportional to the risk. Inappropriate counter-measures risk compromising everybody's lives, every day.

5. ensure that responsibilities and powers are explicit and clear. Legislation is a good method of achieving this aim.

6. security measures must be transparent and accountable.

7. new security measures must have the capacity to be reviewed and, preferably, contain sunset clauses. Beware of legislating away civil rights.

THREAT TO INDUSTRY

Professor Alfred Bullesbach, Chief Officer of Corporate Data Protection at DaimlerChrysler AG, gave an outline and evaluation of worldwide legislative changes in the light of the US attacks, suggesting that they have, broadly speaking, led to increased powers for public authorities around the world. He went on to say that "the special perspective of a Chief Privacy Officer (CPO) within globally operating corporations leads me to emphasise that the disrespect of privacy rights might be seriously harmful to both global free trade ideals and free flow of information. These essentials – serving as the motor developments towards more prosperity – must remain untouched. It is striking that not only the interests of companies are harmed. They of course may fear, with good reasons, that being spied upon in the name of national operations could lead to a loss of valuable company secrets and know-how."

His solutions were to apply a strictly interpreted purpose principle to previously collected data, and to examine the need for protection of internal communications infrastruc-

continued on page 15