EU's Art. 29 group cautious on anti-terrorism legislation

Report by Alan Pedersen

CONCERNED BY SOME GOVERNMENTS' attitude that the protection of personal data is blocking the fight against terrorism, the EU's Data Protection Working Party has called for a comprehensive debate.

Since the September 11th attacks, a whole range of anti-terrorism measures have been discussed. These include stepping up the use of existing technology, for example biometric facial recognition. There is also pressure being applied to communications service providers to retain and disclose Internet and e-mail traffic. It is an issue that not only affects the interest of individuals but also business. Attempts in the UK to make it compulsory for Internet Service Providers to retain personal data could be an extremely costly and difficult task for many struggling providers (see p.14).

The Data Protection Working Party has called for a more measured and long-term approach to the problem, believing that if governments act in haste, their citizens will repent at leisure. Terrorism is not some 'flash in the pan' that can be stamped out in one or two years, it is an ongoing global problem. "Terrorism," says the Working Party, "is not a new phenomenon and cannot be qualified as a temporary phenomenon."

The European Convention on Human Rights covers the rights of individuals to protect their personal data. However, in order to combat crime, exceptions have been made.

The Working Party has, therefore, requested that more analysis be put into proposed legislation and the impact it has on personal freedom. And whilst it understands that some measures threatening individual privacy may be necessary, it believes they should be justified and limited to their purpose. Legislation that does infringe privacy should be made transparent, with clear definitions of the scope, the circumstances in which they will be used, and to whom they will apply.

In a report published in December, the Working Party summed up its views with this comment:

"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."

The EU Data Protection Working Party's comments, published on December 14th 2001, can be found at: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

Facial recognition technology is failing

Does facial recognition technology (PL&B Int Sep 01 p.9) enhance security? Two recent reports from the United States stress the limitations of this technology.

In a January 3rd press release, the American Civil Liberties Union (ACLU) reported the massive failure of facial recognition technology being used on the streets of Tampa, Florida. The press release states that system logs obtained by the ACLU through Florida's open-records law show that the system failed to identify a single individual contained in the police department's photo database.

The police department has acknowledged that the software – originally deployed in June 2001 – has not been actively used since August. The press release also states that logs obtained by the ACLU indicated many false matches between people photographed by police video cameras in one city district and photographs in the department's database of criminals, sex offenders, and runaways. The system made what were to human observers obvious errors, such as matching male and female subjects and individuals with significant differences in age or weight. "Face recognition is all hype and no action," said Barry Steinhardt, Associate Director of the ACLU and one of the report's authors. Steinhardt noted that more controlled studies of facial recognition software – by the Federal Government's National Institute of Standards and Technology, by the Defence Department, and by independent security expert Richard Smith – have found levels of ineffectiveness similar to those in Tampa.

In an article published on November 12th 2001, the *New York Times* referred to a report prepared by Richard Smith and the ACLU about facial recognition devices in use at Logan Airport in Boston. The report concluded that the devices were largely ineffective in identifying terrorists – although they might be helpful in making identifications from a smaller pool of local criminals as they try to flee by boarding planes.

Further information: www.aclu.org/news/2001/n010302a.html.