Special report Big Brother

Privacy and the government

Information commissioner

Office of surveillance commissioners

Privacy and data sharing - cabinet office report, April 2002

Home Office: entitlement cards FAQ

GCHQ

Police

National Criminal Intelligence Service

Police national computer

Legislation

Data protection act 1998

RIP act

Antiterrorism, crime and security act

Privacy campaigns

Charter 88

Liberty

Law that favours disorder

The invasion of privacy is now so great that a legislative rethink is needed, says Simon Davies

Saturday September 21, 2002
The Guardian

In June, the human rights group Privacy International received a disquieting complaint from the mother of an 11-year-old child attending a London primary school. The mother claimed that all children in the school had been electronically fingerprinted for a new library system. The school had not sought the consent of parents, nor had it provided an explanation to the children. The entire population of the school was simply herded en masse toward a fingerprint scanner.

It later emerged that the system employed on her child had been sold to about 1,000 schools, resulting in the mass fingerprinting of as many as 300,000 children from the age of seven. The technique is being used to replace library cards and to increase efficiency of library management. That thousands of young children are routinely fingerprinted for school administration is bizarre enough in itself, but the most surprising twist in this tale is that Britain's data protection laws have little bearing on the practice. Indeed the Office of the Information Commissioner, the official responsible for the protection of information, came out squarely in support of fingerprinting, saying it would "aid compliance" with the law by ostensibly making personal information more secure, and identification more reliable. In the furore that followed, senior staff of the commissioner enthusiastically lined up to publicly "encourage" school to fingerprint their children, arguing that it would be an example of "best practice" in information handling.

It would be difficult to find an issue more central to privacy. The fingerprinting of school children brings out deep concerns about the vulnerability of children to "seductive" technologies of control. Surely any data protection law would substantially limit a practice that in time could creep from administration to school registration and finally to general security and law enforcement. Not so. The Data Protection Act, even in its recently revised form, puts the protection of data before the protection of people. Its chief concern is to ensure that data is collected and maintained properly, stored securely, and used for specified purposes. It does little or nothing to prevent the creation of surveillance.

While the fingerprinting scandal simmered, astute observers of government policy were coming to grips with the realisation that the data protection regime was also going to have little or no bearing on plans to introduce a national entitlement card. The government was clear that the proposals - although constituting one of the most wide-

Liberty

Privacy International

Privacy and human rights report 2002

Statewatch

Online privacy

Cyber-rights and cyber-liberties

Electronic privacy information centre

Online privacy alliance (US)

Credit information

Experian

Electoral roll

192.com

Think tank

Foundation for information policy research

ranging information initiatives of modern times - complied fully with the Data Protection Act. The information commissioner has more or less agreed, arguing only that the information used to form the basis for a card system would have to be accurate.

It can reasonably be argued that the act and the commissioner have become woefully inadequate as guardians of privacy. There exists a systemic failure in both mechanisms to recognise and limit the most dangerous and pernicious invasions of privacy. Public interest exemptions from data protection laws have resulted in wholesale violations of privacy. Governments and private sector organisations have moved - sometimes unimpeded - in recent years to incorporate surveillance into almost every aspect of our finances, communications and lifestyles. While acknowledging the importance of privacy as a fundamental right, those who establish such systems argue that surveillance is necessary to maintain law and order and to create economic efficiency, and that privacy rights in general must remain subject to constraints of fiscal and public interest. This argument is correct in principle, but frequently feeds on hypocrisy, deception and a total absence of any intellectual or analytical foundation, resulting in unreasonable extensions of surveillance.

If the principles of data protection were enforced across the information spectrum (without, for example, broad public interest exemptions), it is feasible that current legislation might offer substantial protection for individuals. However, there are three key factors that prevent this condition from occurring. First, governments generally tend to ensure that the most vital areas of their functioning are at least conditionally exempt from privacy law. Second, individuals - while consistently expressing anxiety - are overwhelmed by the processes required to enforce protection of their privacy. Third, privacy and data protection regulators are frequently fatalistic, timid or under-resourced.

Of course, there have been occasions when the mechanisms for protecting data have in fact succeeded in protecting individuals, but it is rare. In every country, privacy and, more specifically, data protection laws have failed at fundamental levels to protect individuals.

In Australia, limitations on the use of data have failed to prevent an extensive regime of public sector data matching; in the same way, the collection limitation principle in UK law has failed to prevent the breathtaking growth of visual surveillance. Even European data protection laws, arguably the most advanced in recognising the importance of the individual, have done little to prevent the spread of DNA testing, communications interception or the use of identity cards

From time to time, the mechanisms employed to protect our fundamental rights must be reviewed and revamped. For data protection, that moment is long overdue. The principles that form the foundation of data protection are now more than 20 years old, and their legal heritage is ancient. Battered and compromised by changing fortunes and times, stress fractures within the principles are now so prevalent that some areas are at risk of collapse. As a result, the nature and extent of privacy invasion has fundamentally eclipsed the capacity of law to provide limitations and redress.

· Simon Davies is director of Privacy International.

Printable version | Send it to a friend | Read it later | See saved stories