Struggles to defend privacy: challenges from 1950 to 2010

The keynote address at this year's PL&B Cambridge conference was given by Professor Alan Westin, Publisher of *Privacy & American Business* and one of the world's leading experts in privacy and data protection, with experience dating back to the 1950's. His presentation drew the big picture, putting international data protection into a cultural/historical perspective, giving his views on the current agenda then building on this analysis towards predictions for the first decade of the 21st century.

He began by identifying privacy as one of three competing values to be found in every democratic society, the other two being the need for public disclosure of information (particularly official information held by governments) and the need for safeguarding public order, national security and public safety. Of these three values, individual privacy is the most "fragile", and therefore, needs to be nurtured and protected with most vigilance.

The struggle between these values classically takes place in three areas: means of communication (the post, the telephone, or latterly the Internet), record-keeping systems in which information about individuals is held, and government surveillance. Data protection and privacy protection is therefore closely entwined with matters of socio-economics, morality, culture and, above all, legitimacy of behaviour. It is also a critical issue in deciding the role of government in the market place.

Privacy is not an absolute value, but one that is balanced against others. It is also a variable value. Some individuals value privacy more than others. Most of us want to be left alone at times, but want to participate openly in society at other times. Our opinions about privacy also change as we go through different phases of life.

For Professor Westin, the need for privacy is not a constant, but a changing phenomenon, and is ample demonstration that a "one size fits all" approach to privacy protection is misguided.

Data protection in the pre-computer age

During the 1945-1960 period most concepts of privacy were based on 'search and seizure' law, freedom from surveillance and legal concepts of 'due process'. In the US, these concepts found expression in the 1st, 4th and 5th Amendments, in common law duties of confidentiality, and statutory protection for the privacy of the mail.

New developments in communications, such as the telephone or the telegraph, or new record-keeping technologies, such as the typewriter, created expectations of privacy which people were able to claim and exercise.

But the profound social revolution of the 1960's, creating citizens' rights to non-discrimination and equality, required a re-evaluation of this approach. Indeed, it is probable that this social revolution could not have happened without a change in the US approach to its regulation of record-keeping. Against the background of the civil rights movement, data about race, religion, gender, sexual preferences or political opinions became increasingly viewed as a means of discrimination.

At the same time, great technological advances were being made - micro-listening devices, lie-detectors, increased use of psychological testing, and of course the arrival of the computer and information communications systems. This triggered a number of alarms in the US and Europe about the impact of such technological change on the delicate balance between privacy, public disclosure and surveillance. As a result, governments around the world, and some private bodies, undertook studies to evaluate the threat to privacy being posed by these technologies. The result of this empirical research was that although privacy had not yet been eroded, it was sure to be so in the near future, unless a new approach to privacy protection was taken.

The first era of data protection laws

In the US and Europe, pre-emptive responses to the problem took shape. In the US, this became "fair information practices", in Europe it was termed "data protection". The two approaches were, however, broadly the same, encompassing a set of common principles: no record systems should be secret; individuals should know what information was being collected about them; information should be held for specific purposes and with the consent of the individual, unless otherwise permitted by law; a right to see, correct

or challenge one's personal information, some control over disclosures or secondary uses.

These common principles formed the basis of the laws elaborated in the "first era" of data protection regulation. In the US, a federal Privacy Act was adopted in 1974 covering public sector records held by the federal government. Several dozen States followed suit and adopted laws covering the records at state level. In the private sector, however, the "omnibus" approach was rejected in favour of a "sector-by-sector" approach, an early example being the Fair Credit Reporting Act of 1970 which regulates the keeping of credit reports for credit, employment and insurance purposes. It includes a number of important substantive rights, and means of redress and enforcement via the courts or the Federal Trade Commission. Subsequently, sector- specific legislation in the 70's and 80's has been developed in the financial area, electronic communications, cable television and the video rental sector.

In Europe, Sweden led the way with its 1973 data protection law, followed by Germany, France and others as the decade progressed. These early laws, with their requirements for registration or licensing of record keepers, were based on a particular moment in the history of computing. It was a time when the IT industry was dominated by a relatively small number of mainframe computers, run by specific departments within organisations that were effectively the 'responsible keepers' of the computer system. At that time, the data protection laws developed were an exact fit for the technological model of the day.

The second era of data protection laws

The second era, beginning in the mid-1980's, was characterised by massive changes in the nature of computing technology. The PC revolution led to a situation where individuals could possess more computing power on their desktop than was housed in the entire mainframe of early IBM computers which characterised the first era. Autonomous individuals within organisations were now able to run databases on their own machines. Computing had become decentralised. The second main change was in the nature of communication. Individuals became able to "talk" to others over their PCs, sending e-mail to other people who might have no connection whatsoever with the organisation in which the individual worked. Local Area Networks have come to prevail over mainframes.

Other changes took place. Old-fashioned mass marketing (via television, billboard advertising etc.) was increasingly being overtaken by "target" marketing: sending marketing material directly to those individuals who are known to, or might be supposed to, have a specific interest in the product being marketed. Businesses became interested in knowing their customers and, as a result, the collection of personal information and customer profiles has become a major data protection issue.

While these trends were taking place, both the US sector-based approach to privacy protection and the European "omnibus law" approach with national data protection commissions began to spread to other parts of the world - Asia, Eastern Europe, and Latin America.

Reflections on the current period

There are many positive features. Opinion surveys consistently show high levels of public awareness and concern about privacy issues, and particularly about harm that could result from the matching or misuse of government-held data. At the same time, the globalisation of the economy and of data processing systems has led to a spread of data protection laws to increasing numbers of jurisdictions. Another feature is the growing acceptance in business circles that good data protection practices can result in better business practices, contributing to better customer relations and more efficient management of data resources.

The impact of the EU Directive

One topical question is the impact of the EU Data Protection Directive on data flows between Europe and the US. In Professor Westin's view, an accommodation will be found between the two sides. Either the US will be found to have an adequate level of protection (particularly if additional legislation is adopted in the medical sector, and, as President Clinton has proposed, a specific law on genetic data used for insurance purposes is introduced), or data transfers will continue on the basis of safeguards provided by contracts or industry codes. Confrontation is therefore unlikely. In fact, the two sides have much to learn from each other. Europe must learn to adapt its approach to cope with the new technological environment and the challenges of

the Internet (for which the Directive is somewhat unsuited), while the US must take action to improve the remedies available to individuals when rules are breached. Indeed, on the day of the presentation, President Clinton hosted a press conference to launch the *Magaziner Report* on electronic commerce which includes an important policy statement on the use of technology and voluntary standards to guarantee privacy in the on-line world.

There are, however, some negative aspects to the current situation. There seem to be relatively low levels within Europe of public awareness of data protection laws and supervisory bodies. An EU study of a representative sample across the 15 Member States put such awareness at only 30%. Data protection is not exactly a household word in either North America or Europe.

Another disturbing development is the growing public backlash against the Internet, which is increasingly seen as an aid to terrorists, drug dealers and the like, and indeed as posing a major threat to the ability of law enforcement agencies, armed with their traditional search and seizure powers, to track down criminals. This fear underlies the whole of the current debate about cryptography. If government agencies are unable, when justified and subject to proper procedures, to read the content of messages sent on the Internet, then the public should be rightly concerned. And there are other problems - consumer fraud over the Internet, obscenity - together with a general feeling that there is 'too much privacy' on the Internet, all of which causes difficulty to those wishing to ensure that an appropriate privacy balance is maintained in the on-line world.

Data protection into the next decade

A major issue to be addressed in the next ten years will be that of genetic data. The current reaction of distrust, manifested by temporary prohibitions on the use of such information, is the correct one. However, as genetic testing becomes more reliable, such data will become a common part of medical records. In such circumstances, the use of genetic data for life/medical insurance purposes becomes inevitable, as will its use in employment and recruitment. The challenge will be to define the parameters for such uses.

A boon to privacy could be the development and wider use of biometric identification technology. The advantage of such techniques is that they do not require databases against which the identifiers can be compared. Biometrics identifiers are free-standing, and could therefore be privacy-enhancing.

Smartcards for electronic cash may or may not be positive for privacy. Multi-use cards are very convenient, but how secure are they? How much control will there be over access to the data held on the cards or the system with which they interact? The potential to facilitate anonymous financial transactions leaving no identifiable data trail could be very positive for privacy.

As far as the Internet is concerned, off-line problems will continue to be replicated on-line. The Internet will continue to grow in importance with ever-increasing amounts of commerce and communication taking place in Cyberspace. Public data becomes more readily available and searchable over the Internet than ever before. This creates a new problem, which we are already seeing in the burgeoning number of "look-up" services being offered on-line, which search the Internet to compile detailed profiles on named individuals, the data being made up predominately of publicly available information.

The best responses to Internet-based privacy problems will mix technological tools with industry codes and standards that are certified in different ways. (The current TRUST-e initiative is an example of this approach.) These ideas will develop over the years. New legislation of privacy on the Internet is not yet appropriate.

Conclusions

Privacy values are very similar throughout the world, but just find different forms of expression and different legal and social regimes from country to country. The new IT revolution can return a great deal of power to individuals, providing a great opportunity for them to be able to demand and receive the level of privacy they desire. Each person has, in effect, the potential to become his own data protection commissioner. There is no reason why this should not become a reality. Electronic commerce depends on the trust of consumers. Market mechanisms could therefore support more rather than less privacy. This is a cause for optimism.

Report by Nick Platten independent consultant.