United States searches for a privacy policy to include Internet and EU Directive

The National Telecommunications and Information Administration, better known as NTIA, is part of the Department of Commerce and advises the President on telecommunications and information issues. NTIA thus has responsibility for formulating policy on behalf of the President with respect to private sector information practices. In this edited extract from her *Privacy Laws & Business* 1996 Annual Conference paper, Barbara Wellbery, Chief Counsel at NTIA, outlines the issues.

Balancing the free flow of information against an individual's right to privacy is not a new issue in the United States. Over a century ago, one of our most noted jurists, Louis Brandeis, wrote: *Recent inventions and business methods call attention to the next step which must be taken for the protection of the individual and for securing to the individual,... the right to be let alone.* At the time this was written, the issue of the day was the tabloid press. Over a century later, we are still wrestling with the issue of privacy, trying to find the right balance.

Technology now allows data to be stored, transmitted, sorted and compiled at ever-increasing speeds and decreasing costs. Information that once took days, if not weeks to collect and compile, now takes minutes.

The Internet has the potential to increase risks to privacy geometrically. The risks become clearer when we realise that use of the Internet leaves in its wake information trails: our mouse clicks can be tracked, and marketing profiles compiled, using our so-called "mouse droppings" - places where we have stopped to browse on the Net. These need not just be commercial applications, but also, for example, which political bulletin boards we have visited.

Privacy in the USA - the core elements

Privacy has always been important to the people of the United States. We share the European concern about data protection and the heightened risks that the Information Age poses. And, I believe, in the United States, for the most part, we share with the European Union, consensus on the general substantive principles applicable to fair treatment of personal information by the private sector.

Specifically, many agree that information users who collect personal information should provide notice about why they are collecting information, what the information is to be used for and how its confidentiality, integrity, and quality should be protected. We also believe the data users should obtain customer consent before using any personal information. The precise requirements and interpretation for these standards may well differ, but I believe the core elements are commonly accepted on both sides of the Atlantic.

The Clinton Administration also believes that information privacy is critical to the development of the Information Superhighway. The concern is that individuals will be reluctant to participate in the Information Age if they are afraid that their personal information could be used for purposes which were unintended, embarrassing, harmful or improper.

We do differ from the European Union, however, in how we would go about minimising risks to privacy. And these differences stem at least in part from our very different traditions and our very different legal systems.

United States legal tradition

In the United States, we look to the Constitution for our fundamental rights, and there is no explicit right to privacy in the United States Constitution. United States courts have, however, ruled that the Constitution extends to citizens an implied right to certain forms of privacy. For example, the Supreme Court has held that the Fourth Amendment affords individuals freedom from Government intrusion into their physical space by imposing limits on searches and seizures by law enforcement officials. State constitutions also protect civil liberties in a manner similar to the Federal constitution. And at least one state constitution, California, does include an express right to privacy.

But the United States Constitution has never been read to protect information policy, and it is also noteworthy that neither the United States Constitution, nor other state constitutions, proscribe the activities of non-governmental

actors, i.e. private sector companies. These constitutions govern only government action.

Limiting government

This distinction between limiting government but not private sector action, is consistent with American political philosophy, which has at its core a belief in limited government, particularly at the Federal level. Even though the role of the Federal Government in United States society has increased significantly in the last 60 years, a good deal of antipathy toward government regulation of private relations endures. The prevailing view is that the Federal Government should not intervene in the marketplace in the absence of compelling needs. Federal legislation is generally remedial in nature rather than prophylactic.

Specific and highly targeted privacy

In addition, the United States' approach to protecting privacy has been targeted to address sectoral issues, rather than to overhaul broad areas of the law.

Even on those occasions when the United States Federal Government has reacted to egregious misappropriations of personal information by passing laws that constrain the private sector's use and collection of personal information, these laws have not, as is often in the case in Europe, taken an omnibus approach to privacy. Rather, they have focused on specific instances of abuse in specific sectors of the market.

To provide just one example, the Federal Video Privacy Protection Act, which regulates the use of personal information collected in connection with video sales and rentals, was passed in reaction to the use of information about Judge Bork's video rentals to defeat his nomination to the Supreme Court.

The law is limited, however, not only in that it affects only a limited industry sector - video rentals - but it also appears to apply to one form of video rentals only, hard copies, and not, for example, to electronic copies, as for example, those provided when movies are rented over a telephone line, as is now possible.

Encouraging private sector guidelines

Consequently, the general tendency in the United States is for fair information practices to be created and enforced through industry self-regulation. A number of United States trade associations have promoted fair information practice guidelines for the treatment of personal information in specific industries. Many individual companies have also established policies and practices, including internal codes of conduct and procedures, to protect consumer information.

The Clinton Administration believes the Federal Government has a number of important roles to play in the area of information privacy as well. Of course, we have a primary role in ensuring the privacy of the information that the Federal Government collects and uses. In addition, the Clinton Administration recognises that the success of the Information Superhighway depends on individuals' ability to safeguard their personal information. Therefore, it has taken the initiative in developing policies designed to do that. These policies encourage private sector rather than government implementation, however, and view legislation at the Federal level as a last resort for if, and when, the private sector fails to act.

Avoiding bureaucracy

It is also worth noting that the United States does not have one centralised privacy office at the Federal level. The idea of having a centralised supervisory privacy body with regulatory power is quite foreign to the United States; from our perspective, the existence of such a body could perhaps itself be viewed as leading to potential invasions of privacy. Rather, United States Government privacy efforts are diffuse and located in a number of Executive Branch agencies, as well as in independent regulatory Federal agencies. At the state level, various state agencies may have a role in privacy, for example, state attorney generals' and consumer affairs' offices.

NTIA's Privacy Report

In February 1994, the NTIA issued a Notice of Inquiry on the use of personal information in the telecommunications and information industries. In October 1995, the NTIA published a White Paper entitled *Privacy and the NII: Safeguarding Telecommunications Related Personal Information.* This paper looks at privacy concerns in the context of the telecommunications and information service sectors and specifically those concerns that

arise in connection with an individual's subscription details and use of telecommunications and information services, information that we call *transactional data*. The White Paper attempts to strike the proper balance between the interest in the free flow of information and the individual's right to privacy.

NTIA concentrates on transactional data

We concentrated on transactional data in the White Paper, because we thought the area needed greater attention and protection in the United States - it appeared people did not realise how much can be revealed about individuals just from the subscription information they provide when they take a new service - for example, names, telephone numbers, service preferences - and when they use the service - who they call, how long they talk, what web sites they visit - all without even looking at message contents.

Privacy laws in place in the United States are limited in scope and may be inconsistent in application. They are generally confined to a specified group of existing services and do not apply to all providers of any one service. Further, they may not readily apply to many of the next generation of services and may not be adaptable for that purpose. In fact, responses to our Notice of Inquiry and our research indicated that there are gaps in company information policies and in how existing privacy laws and regulations treat personal information generated by subscription to and use of telephone and video services. In addition, transactional data generated by use of the Internet receives almost no protection. NTIA, therefore, concluded that remedial action was warranted.

NTIA's proposed framework builds upon the work done by the Organisation for Economic Co-operation and Development (OECD), the responses we received from our Notice of Inquiry, and on work done by an Administration working group, namely the report prepared by the Privacy Working Group of the Information Infrastructure Task Force, entitled: *Principles for Providing and Using Personal Information.*

NTIA's self-regulatory approach

We proposed a self-regulatory framework that has two fundamental components

1. provider notice and
2. customer consent.

Notices would include information about

- why a company is collecting information,
- what it will be used for, and
- how its confidentiality, integrity, and quality will be protected.

Under this framework, telecommunications and information service providers would also notify individuals about their information practices, adhere to those practices, and keep customers informed of changes to such practices. Service providers would be able to use information collected for stated purposes once they obtain consent from the consumer. Explicit or affirmative consent would be needed for sensitive information; tacit consent would be sufficient to authorise a firm to use other information.

Sensitive information

Although the White Paper did not definitively define sensitive information, we did identify some clear examples:

- political persuasion,
- health care,
- sexual matters, and
- personal finance.

The report also emphasised the need for consumer education so that consumers will have more control over how their personal information is used and will be able to see the ways it can be used beneficially.

Action if self-regulation inadequate

One premise of our report is that consumers will benefit from uniform, minimum, effective privacy standards that apply to like services. Such standards will also reduce a potential barrier to consumer use of the Information Superhighway. Voluntary privacy requirements will also benefit the private sector by eliminating a potential source of competitive advantage or disadvantage among rival providers of like services. At the same time, a self-regulatory approach gives companies flexibility in discharging privacy obligations and thus the opportunity to do so in a way that minimises costs to the organisation and society. We believe our recommended approach should adequately protect the individual's legitimate

privacy interests without excessive government intervention in the market place.

NTIA is working with telecommunications and information companies to gather information on company policies on privacy protection and to see whether they are implementing changes as a result of recommendations in the White Paper or for other reasons. *If, however, industry self-regulation does not produce adequate notice and consumer consent procedures, we believe government action will be needed to safeguard privacy interests of American consumers.*

Regulating the Internet may stifle its growth

This self-regulatory approach is also consistent with the Clinton Administration's approach to regulating the Internet. The Administration's consistent policy on the Internet has been that it should be allowed to evolve with minimal government regulation and intrusion. The growth of the Internet to this point has been phenomenal. It has been successful beyond anyone's wildest dreams and continues to evolve, sometimes it seems, almost on a daily basis. In the United States, much of this success is attributed to the lack of government regulation. We are concerned that government regulation could have the undesired effect of stifling the Internet's growth.

Furthermore, the international nature of the Internet - the irrelevance of physical boundaries - makes regulation of the Internet and enforcement very difficult. There is no way of preventing electronic materials that originate abroad from entering another country. It is also not clear that governments have the power to enforce regulations against foreign entities whose only contact with the jurisdiction is over the Internet. And thus, national legal requirements may have little or no effect on such material.

Consumers to choose their privacy level

The Administration, therefore, looks to industry self-regulation solutions to address privacy (as well as other) issues arising from Internet use. The online industry has already begun self-regulation to enhance privacy. Microsoft has adopted very stringent practices for online data protection. And AT&T and MCI are now marketing their services to consumers by promising a commitment to ensuring that customers receive adequate privacy protection.

The Clinton Administration also favours technological approaches that would empower consumers to control access to information. One promising approach would take the Platform for Internet Content Selection technology (PICS) developed to empower parents to prevent their childrens' access to violent or otherwise inappropriate programming, and adapt it to prevent access to web sites that did not provide the specific level of privacy desired by a consumer. The advantages of technological solutions include eliminating the need for government regulation and allowing consumers to custom tailor their desired level of privacy protection.

The European Union Data Protection Directive

From our perspective, one of the most controversial aspects of the Directive is its requirement that Member States enact laws to prohibit the transfer of personal data to third countries that fail to ensure an "adequate level of protection" for personal information. [Art. 25(1)] As a result of this provision, the Directive and the implementing laws of Member States could have enormous consequences for United States companies with European operations, as well as United States companies that use the Internet.

> "If, however, industry self-regulation does not produce adequate notice and consumer consent procedures, we believe government action will be needed to safeguard privacy interests of American consumers."

Does the USA provide adequate protection?
A European Union Working Party has been set up to review the laws of third countries and to determine which countries do not provide adequate data protection. We are concerned about how the European Union will determine whether or not a third country's privacy policies are adequate.

Although the Directive provides that the adequacy of the protection offered is to be assessed in the light of all the circumstances, including the nature of the data, the rules of law, and the professional rules and security measures that are complied with in that country, we are concerned because the specific criteria that will be used to judge the adequacy of protection in third countries have not yet been formulated.

If the European Union determines that the United States does not provide adequate privacy protection, American businesses that use personal data collected, stored, or processed in Europe, and American companies with operations in Europe, may be unable to move data legally to the United States. Those United States companies could be required to establish separate data facilities in the European Union for their European operations.

"We are concerned about how the European Union will determine whether or not a third country's privacy policies are adequate."

To help ensure that the European Union analysis of United States privacy protection is comprehensive, NTIA recently served as the contact point for the European Union, and hosted meetings with European Union representatives, other United States Government agencies and the private sector, to begin to discuss our respective privacy approaches, laws, and regulations.

The USA/EU dialogue continues

In addition to the United States/European Union bilateral discussions in March, we had two meetings with Mr. Brühann, the Head of Unit responsible for Data Protection at DG XV at the European Union, and other meetings with Federal Government and private sector representatives. These meetings were good, open discussions, in which we tried to understand the other's perspective and approach to data protection.

The European Union specifically asked us to focus on direct marketing, credit reporting and medical data. We also took the opportunity to explain the United States approach to privacy, as well as contractual and possible technological solutions to protecting information privacy.

We were encouraged by those meetings. United States companies were able to demonstrate their concern for the privacy of personal data as well as their ability to protect such data. It became clear that there exists a shared willingness to engage in a continued, productive dialogue.

How will adequacy be determined?
We remain concerned, as do many American companies, about how adequacy will be determined and whether self-regulatory and contractual approaches will be considered by the European Union in making its determinations. American companies have expressed some concern to us that simply not knowing how adequacy will be evaluated creates planning problems.

NTIA offers contact role

It also became clear to us that we need to know how Member States are implementing the Directive and more about their approaches to fair information practices. We plan to continue our discussions during both formal and informal meetings between the United States and the European Union and to meet with representatives from Member States in the near future.

We hear occasionally from visitors to the United States that they are at a loss as to who to talk to about privacy issues, since the United States does not have a centralised data protection agency. The National Telecommunications and Information Administration, working with the Department of State, would be happy to serve as the point of contact for your visits.

Barbara Wellbery, NTIA Chief Counsel, addressed the 9th *Privacy Laws & Business* Conference at St John's College, Cambridge in July 1996. She may be contacted at National Telecommunications and Information Administration, U.S. Department of Commerce, Room 4713, 14th and Constitution Avenue NW, Washington D.C. 20230, U.S.A. Tel: +(1) 202 482 1816 Fax: +(1) 202 501 8013