Data protection in the United States - a rising tide?

While the USA has no comprehensive data protection legislation, American consumers believe that strong measures must be taken to protect privacy. An opinion poll showed that 58% of the public want a privacy law now. Marc Rotenberg challenges President Clinton's support for self-regulation (PL&B Aug 97 p22).

American consumers and Internet users have consistently expressed concern about the loss of privacy, and have consistently shown support for new legislation to protect privacy. It is recognised that law is often an imperfect solution, but there is also a strong belief in the rule of law. By tracing the development of privacy law in the United States over the twentieth century, it can be seen that the United States has always shown great regard for the right of privacy and expressed widespread concern when privacy was at risk. So, when I say that privacy is a great concern in the United States and that we need to do much more to protect it, I do so with the newspaper stories piled high, the polling numbers unambiguous, and with a respect for history that makes clear that few rights in American life are more greatly valued than the right to protect private life.

Public support stronger than ever before

There are three central issues that need to be addressed to build a bridge between the United States and Europe. These issues are: current attitudes of consumers, government policies on self-regulation, and enforcement. If the USA can successfully address these issues, we can enter the information society together with mutual standards that protect the privacy rights of our citizens.

The first issue concerns current attitudes of consumers in the United States. It is clear the consumers and users of the Internet favour the passage of law to protect personal privacy. Professor Alan Westin (PL&B Oct '97 pp. 20 - 22) found this year that 58% of the American public want the government to pass a law to protect privacy now, and 24% said that the government should formally recommend privacy standards. Only 15% favoured letting groups develop voluntary privacy standards and the government taking action only if real problems arise. Professor Westin's results are consistent with other surveys of attitudes toward privacy in the United States. A 1991 poll conducted by *Time Magazine* found that 93% of the US public felt that companies that sell personal information to others should be required to obtain explicit permission. And the most comprehensive poll of Internet users ever undertaken found that users of the Internet in the United States, on a 1 to 5 scale, said that the Internet needs new laws to protect privacy at a level of 3.8.

Congress introducing bills on privacy

It is clear that some political leaders favour the adoption of privacy law. While it is true that the White House has expressed the opinion that privacy legislation is unnecessary at this time, members of Congress are of a different opinion. Bills have been introduced in the House and the Senate that address a wide range of privacy issues.

One bill would limit the disclosure of Social Security Numbers. Another bill would prohibit Internet Service Providers from disclosing customer information without consent. A third bill restricts the ability of direct marketers to sell information about young children. Several bills have been introduced to address public concern about unsolicited commercial e-mail, and many other bills are also under consideration. Also, several laws have been introduced in a little over a decade that specifically target new technologies: cable subscriber records were covered in 1984, electronic mail in 1986 and video rental records in 1988. Even junk faxes and auto-dialers became subject to privacy legislation in 1991.

Self-regulation has failed

The view of some that the United States does not support the passage of privacy legislation is clearly not supported by the majority of people in the United States, many of our elected officials, or our recent history.

Much has been said recently in support of self-regulation. Self-regulation has been offered as a privacy solution, a way to steer a course between government control and free market chaos. The current argument for self-regulation is based on a preference and not a principle.

While much has been said about the "common philosophy" of the Administration's policy

towards the Internet, it is quite clear, some would say painfully clear, that the Administration is prepared to regulate if the interest at stake is copyright or cryptography.

Self-regulation as an argument against privacy protection is hardly new in the United States. The direct marketing industry has argued for more than twenty years that it did not need privacy regulation. The result is that Americans receive a flood of junkmail, more junkmail per capita than any other country in the world. Millions of Americans sign up for the Mail Preference Service to escape this onslaught, but there is no assurance that the privacy of these people will be protected. Professor Joel Reidenberg and Professor Paul Schwartz have shown, in their study of data protection in the United States (p.18), that the Mail Preference Service is ignored by about half the members of the Direct Marketing Association.

Self-regulation has also failed repeatedly in the last few years as trade groups and individual companies have been unwilling to uphold their own principles and their own contractual agreements.

Asymmetric effects of self-regulation

Advocates for self-regulation have redefined privacy in a way that is ultimately harmful to the interests of consumers. Instead of focusing on the obligations of the organisations that collect personal information to safeguard the information and use it only for appropriate purposes, the self-regulatory environment has produced numerous proposals that all share the common goal of extracting as much information from the individual as the individual can be coerced to give up by means of contract.

A typical negotiation in an environment produced by P3 (PL&B Oct '97 p.28) or OPS (OPS is Open Profiling Standard, similar to P3, which allows the user to control the release of their data in a secure manner) requires consumers to satisfy the information disclosure requirements of the business as a condition of gaining access to services. As my colleague Professor Agre has observed, these relationships easily become asymmetric with the organisation having the greater power to control what information about itself is released, while simultaneously obscuring the nature and scope of the information it has obtained about individuals.

Of course, one remains "free" to withhold consent, and therefore to be denied admission to a web site, or service from a web-based company, and many other opportunities in the Information Society, regardless of whether a fair justification for the data collection is provided. Simply, self-regulation elevates the principles of notice and consent to stratospheric heights, and ignores most other principles of privacy and data protection.

Self-regulation has also given rise to the emphasis on a multiplicity of privacy preferences. But whether individuals actually have such diverse privacy preferences, particularly in routine commercial transactions or in data gathering activity remains to be seen.

Self-regulation has a further problem: it provides a very limited view of the problems surrounding privacy protection. It focuses on the microeconomic relationship between buyer and seller and ignores the larger social questions of architecture and design. Should highway systems be designed with anonymous toll payment? Which technologies could facilitate commerce and protect privacy? What stand should governments take on the use of cryptography? Self-regulation provides no answers to these questions; it provides no mechanisms to find solutions.

FTC - a history of failure to enforce

It has been proposed that the Federal Trade Commission could enforce a self-regulatory privacy regime by prosecuting deceptive trade practices (PL&B Sept '96 pp. 2-7). But the FTC's ability to actually enforce privacy protection in this manner is highly suspect. First, the legal authority of the FTC under Section 5 of the Federal Trade Commission Act typically requires a showing of "actual harm" to consumers. As those who have studied privacy law in the United States know, this will be a difficult test to satisfy.

But even if this problem is overcome, one could well ask why the FTC, if it had such legal authority, pursued only one privacy case after two years of intense privacy investigation? And in the single case that the FTC investigated, the Commission issued an opinion only after the company had discontinued the challenged practice. There was no actual judgement against the firm or any sanction imposed.

Finally, what expectation can there be that the FTC will pursue any privacy actions in the near future when the Commissioner responsible for privacy matters has now left the Commission? One can look to the Federal Trade Commission for the enforcement of privacy safeguards on the Internet, but you will see only an empty chair.

A violation of competition law

Finally, there is a significant legal objection to self-regulation as a means to protect consumer privacy in the United States: such an arrangement could be impermissible under anti-trust law. It is, as one commentator has noted, a violation of competition law for businesses in the same market to combine to set the terms of competition and then to enforce those terms on their competitors. Establishing industry-wide privacy standards could have exactly this consequence.

Some commentators have suggested that it may be possible for such agreements to survive anti-trust scrutiny if the codes are sensibly designed and do not discourage competition. But drafting such a policy may not be so simple. What happens, for example, if industry adopts a code based on an opt-out procedure, and an innovative company, recognising the need for a higher privacy standard, prefers to offer an opt-in procedure instead? If the industry association discourages the company from offering the higher standard, consumers would be harmed and an anti-trust action could result. Indeed, there is already anecdotal evidence that the marketing industry has engaged in just such practices.

Self-regulation provides neither the assurance of a legal right nor the innovation and competitive benefit of the marketplace. It is simply an answer to the question: how do we regulate without the government ? This is not a path to privacy protection, it is not even privacy policy.

Internet protocols a basis for privacy?

It seems to me surprising that we are unable today to resolve the privacy differences between Europe and the United States particularly as they concern the Internet. Both regions share a high regard for privacy and a long privacy tradition. Both regions seem eager for greater privacy safeguards. The Internet offers the ideal environment to establish uniform standards to protect personal privacy. This is clear to anyone who recognises that the platform is consistent around the globe, that the protocols are consistent, and the customs surrounding commercial transactions off-line are surprisingly consistent: money buys products and services, the disclosure of one's address is necessary to receive delivery of goods, and the release of personal financial information may be necessary when credit is sought. For the vast majority of transactions on the Internet, simple, predictable, uniform rules offer enormous benefits to consumers and businesses.

It is clear what the goal is. We must find a way forward. The European Commission would have ample justification at this point if it decided to restrict certain data flows to the United States because of the absence of appropriate privacy safeguards. How can this point be disputed? Consumers in the United States know that we lack adequate privacy protection. The United States should move quickly to establish a privacy agency, and then proceed to explore the application of the OECD Privacy Guidelines to the private sector. This useful framework provides a strong foundation for the development of technical means to protect privacy and the development of new privacy standards and legal safeguards. It is already found today in several US privacy laws and in the practices of many US companies.

International privacy convention needed

I also propose that the United States, Europe, and Asia join together to develop an international convention on privacy protection based on the OECD Guidelines. A simple framework of general goals, combined with a consultative process that brings together a wide array of countries, could help ensure that privacy standards are extended around the globe.

It is also my hope that, in the process of working together toward a common goal, some of the current differences between the United States and Europe will diminish. There is too much at stake for consumers, citizens, and users of the Internet to risk a clash of privacy rules.

Privacy advocate, Marc Rotenberg, gave this edited presentation at the 19th International Conference of Data Protection Commissioners in Brussels, September 1997. He is Director of the Electronic Privacy Information Center in Washington DC, USA. Its website is at: http://www.epic.org