Consumer privacy in the information age: a view from United States FTC

US Federal Trade Commissioner, Christine Varney, explains the FTC's Consumer Privacy Initiative relating to on-line services, privacy enhancing technology, the collection of data from children on-line, advertising, marketing and telecommunications data, medical, insurance, banks and credit records. Marking a sharp contrast with the comprehensive approach of the EU Data Protection Directive, she says that "The government should step in to regulate only when there has been an identifiable market failure or where an important public policy goal cannot be achieved without government intervention." She concludes that "a robust, competitive marketplace for privacy protection may very well develop. Under this scenario, the market itself could serve the same function as a privacy entity."

The FTC's regulatory role

The US Congress created the Federal Trade Commission in 1915 to promote a free market economy. While the FTC shares joint responsibility with the Department of Justice for U.S. competition policy and antitrust law enforcement, we are the principal regulatory force at the federal level to protect US consumers from unfair and deceptive business practices.

Currently, much of an individual's personal information can be legally collected, shared, exchanged, sold, and disseminated without notice to or input by the individual. Self-imposed industry codes of conduct are increasingly being implemented to address these privacy problems. Critics argue, however, that voluntary codes of conduct are unenforceable. In addition, privacy laws that were adequate when enacted may have become obsolete or ineffective with the passage of time. In short, the time has come for us to consider whether the existing arrangement properly balances individual personal privacy values with competing information flow benefits.

Transactional data trail poses privacy risk

Increased use of the Global Information Infrastructure (GII) for commercial transactions will generate vast quantities of data that can be easily and cheaply stored, analysed, and reused. This transactional data trail poses an incredible risk to personal privacy.

In June 1995, the Clinton Administration's National Information Infrastructure Task Force (NIITF) Privacy Working Group issued an important document entitled *Privacy and the National Information Infrastructure: Principles For Providing and Using Personal Information.*[1] The NIITF Privacy Principles identify three fundamental values that must govern the way in which personal information is acquired, disclosed and used on the Internet:

1. An individual's reasonable expectation of privacy regarding access to and use of his or her personal information should be assured.
2. Personal information should not be improperly altered or destroyed.
3. Personal information should be accurate, timely, complete, and relevant for the purposes for which it is provided and used.

Responsible information gathering

Those who gather and use personal information should recognise and respect the privacy interest that individuals have in personal information by:

- assessing the impact on privacy in deciding whether to obtain or use personal information
- obtaining and keeping only information that could be reasonably expected to support current or planned activities
- using the information only for those or compatible principles.

Further principles were added to these three fundamentals:

Individuals need to be able to make an informed decision about providing personal information. Businesses that collect information should, therefore, disclose the following information:

1. the reasons for the collection of the information

[1] Visit http://www.iitf.nist.gov/ipc/ipc-pubs/niiprivprin_final.html (June 6, 1995).

2. what they expect to use the information for
3. what steps will be taken to protect its confidentiality, quality and integrity of information collected
4. the consequences of providing or withholding information
5. any rights of redress that are available to individuals for wrongful or inaccurate disclosure of personal information.

Businesses that gather personal information should take reasonable steps to prevent improper disclosure or alteration of information collected, and should enable individuals to limit the use of their personal information if the intended use is incompatible with the notice provided by collectors. Information gatherers should educate themselves, their employees, and the public about how personal information is obtained, sent, stored, processed, and protected, and how these activities affect individuals and society.

The NIITF Working Group that issued the Privacy Principles last year acknowledged that the Principles are extremely general and cannot apply uniformly to all sectors. Rather, the Principles are intended to provide the framework from which more detailed guidelines can be tailored to specific circumstances.

The FTC's consumer privacy initiative

Responding to the NIITF Working Group's challenge, the FTC undertook what has come to be known as the Bureau of Consumer Protection's *Consumer Privacy Initiative.*

The Bureau is currently engaged in a dialogue with industry and consumers to develop more robust and specific guidelines for the use of personal information generated by on-line commercial transactions. The goals of the *Consumer Privacy Initiative* are to foster development of a competitive marketplace for privacy protection, assess the effectiveness of a market-driven privacy system, to participate in the policy-creation dialogue, and to enact regulation or recommend legislation if and when such government acts become necessary.

Federal regulation only if market failure

The government should step in to regulate only when there has been an identifiable market failure or where an important public policy goal cannot be achieved without government intervention.

The pace of change in the information industry is unprecedented. Government regulation, on the other hand, moves very slowly, and the predictive skills of government agencies are notoriously limited. As a result, regulatory and legislative solutions to consumer protection issues are unlikely to be either timely or sufficiently flexible with respect to the digital world at this juncture.

The electronic medium itself offers new opportunities for consumer education and empowerment, which, in turn increases the likelihood that self-regulatory regimes can be effective.

These three assumptions lead me to the conclusion that the government ought to move cautiously in the electronic arena.

The government's primary focus at this point should be to support the growth of self-regulatory efforts and on-line education for the public. Internet commerce will not really take off until consumer confidence in the system is established. Hence, it makes business sense for industry to invest in self-regulation and consumer education.

FTC Workshop

As part of this Privacy Initiative, the FTC held a two-day workshop in June 1996 to provide industry, privacy advocates and consumer groups a forum to express their ideas for self-regulation and the use of technology to ensure consumer choice.

The FTC was informed of many industry codes of conduct and standards, including new codes such as the anti-spamming policies (to stop the sending of massive amounts of unsolicited e-mail) issued jointly by the Direct Marketing Association and the Interactive Services Association. The workshop discussed existing codes that are now being revised to comply with the NIITF Privacy Principles. It also examined the familiar fair information practices in off-line settings and asked how these principles would be different in the on-line medium.

Two important areas were explored: the use of medical and financial information on-line. Inevitably, the privacy workshop also discussed international implications of US regulations or industry standards, including the impact of the European Union's Directive on the Protection of

Personal Data. What does the EU Privacy Directive require of US businesses? Can industry satisfy the EU's Privacy Directive's "adequacy" requirement through the use of voluntary privacy regimes?

Choices and costs of privacy

One of the focuses of the workshop was on policy-making. A key issue was what choices should a consumer have about how personal information is used and in which ways can the security and accuracy of personal information be assured on-line?

A second issue involves an acknowledgement that there are costs to privacy. We are all familiar with the old opt-in versus opt-out debate: should we as a society permit businesses to use personal information unless and until the individual affirmatively "opts-out" or should we require businesses to receive an individual's permission prior to gathering her personal information, in other words, the individual must "opt-in." Should the burden of on-line privacy protection be placed on industry or on the individual?

Education, empowerment and self-help

What emerged from the FTC workshop were repeated themes relating to "notice and choice," the two E's (education and empowerment), and emerging self-help mechanisms soon to be available to the consumer.

Panel members, including industry representatives and privacy advocates, seemed to converge on these three privacy principles, at least for this stage of the Internet revolution. While industry representatives urged a 'wait and see' approach by the federal government on Internet regulation, privacy advocates were more cautious about the notion of industry self-regulation without legal remedies.

Technologies give consumers choices

The workshop also introduced existing and emerging privacy technologies that would empower the consumer on-line. At our hearings, software developers demonstrated some highly innovative technologies. One of these was the Platform for Internet Content Selection (PICS), technology which would enable the consumer to define for herself the privacy level she desires. This could be based on Web content, transaction type, services rendered in return for relinquishing personal information, and the uses to which that information would be applied. For these technological solutions to be effective, consumers and industry must be aware of their respective rights and responsibilities with regard to the use of personal information in on-line transactions.

I am extremely optimistic that these strategies will enhance consumer privacy without the need for bureaucratic intervention.

Collection of on-line data from children

The following day, we focused on the collection of data from children on-line. The panel started with a factual finding of what information is currently collected about children on-line and how it is being used. We then moved to a discussion about whether limits should be placed on on-line collection and use of personal information about children. This is a pretty hot topic in Washington these days. The FTC recently received a petition from the Center for Media Education calling for an investigation of electronic advertising aimed at children and the collection of data from and about children on-line. It is clear that there is a need for government, industry, and the public to reach some consensus about the legitimacy of consumer "choice" when the consumer is a child. FTC staff are now preparing a report on the workshop, and I would like to hold follow-up hearings at the end of this year or early next year.

The direct marketing and advertising industries in the US have been tremendously co-operative in this area and appear to be genuinely committed to developing and implementing self-regulatory codes. To the extent that this commitment is carried out, I believe it is premature to regulate the newly emerging world of on-line commerce.

Congressional and industry initiatives

The government and the private sector have become more active with respect to privacy in recent years. Congress is debating several statutory solutions to problems associated with medical information, the collection of data from and about children, communications privacy, and consumer privacy issues arising, or expected to arise, in connection with electronic commerce.

At the FTC privacy workshop, several companies demonstrated impressive technology

that consumers can, or will soon be able to use to protect personal information on-line.

Likewise, trade associations representing the advertising, marketing, and on-line services industries announced new or revised privacy codes and consumer education programs for the information age.

Similarly, NTIA recently issued a White Paper on telecommunications privacy, and is now meeting with telecommunications providers to determine if they are adhering to the privacy principles outlined in the report.

Why are such initiatives under way now? There are a number of explanations for this phenomenon. First, the GII has made it easier to collect, analyse, and distribute data. At the same time, government and consumers are not only becoming more technologically savvy but are also more aware of the data-gathering capabilities of electronic media. As a consequence, greater government and consumer demand for privacy enhancing products and policies has emerged. This can be viewed as an example of the free market in operation.

Privacy of medical records

Currently, there is no federal legislation which directly protects the privacy of medical records.

1. Most observers agree that traditional doctor/patient confidentiality concepts will not adequately protect health-related data in the information age. Increasingly, medical care is provided in a networked environment, and information is readily available to a large number of health care professionals.[2]
2. Doctor/patient confidentiality does not protect medical product purchase data or information provided by patients to third parties.
3. The pharmaceutical industry relies heavily on medical data to evaluate drug efficacy and to promote new product development.
4. Schools, justice systems, employers and the media have access to individual medical information.

Responses, both voluntary.....

As a result, a number of private organisations in the health care industry have promulgated model health information codes that apply beyond physicians. Large physician networks, for example, have established security policies and provided for audits to ensure confidentiality. At the behest of the FTC, the Medical Information Bureau (MIB), which collects medical and other consumer information on 15 million Americans for life and disability insurance companies, voluntarily agreed to provide free copies of reports to consumers who are denied insurance coverage on the basis of an MIB report.

....and regulatory

On the regulatory front, members of Congress have introduced and gained considerable support for legislation to protect personally identifiable medical information without limiting legitimate access to aggregate data.[3]

The Clinton Administration has endorsed a medical privacy bill, although it appears unlikely to come up for a vote before the elections in November this year. Meanwhile, a number of states, including Massachusetts and Wisconsin, have adopted medical records privacy acts. A number of model codes and model statutes have also been promulgated.

2. Quebec's experiment with "smart cards" (cards with computer chip memory which can store identification, financial, insurance, and medical information) demonstrate the benefits of the free flow of medical records among health care providers. Smart cards are being used in limited circumstances in the United States. *See Smart Cards Change the Way We Do Business,* Government & Education, U.S. WEST Publication (1995) or visit http://www.w3.uswest.com/GV/articles/smart2.htm; *see also* Richard Mitchell, *The Public Awaits the Debut of Smart Cards*, Credit Card Management, Feb. 1996, at 59-60.

3. Several bills are currently pending in the Senate and the House relating to the confidentiality of personal medical records. *See, e.g.*, S. 1360, 104th Cong., 1st Sess. (1995) (Medical Records Confidentiality Act of 1995); H.R. 435, 104th Cong., 1st Sess. (1995) (Fair Health Information Practices Act of 1995). For a list of other Congressional bills currently pending see the separate FTC's *Appendix of Current and Pending Legislation on Privacy Rights and Technology.*

Financial privacy without regulations

The Right to Financial Privacy Act[4] limits government access to bank records. However, financial records generated in the course of a banking relationship belong to the bank, and they are not statutorily restrained from reselling the information. Although individual banks have policies with respect to data collection and distribution to non-government buyers, no industry-wide privacy codes are currently in place.

For the moment, the privacy practices of commercial banks seem to be constrained by high consumer sensitivity about disclosure of financial records and the degree of competition that exists in the banking industry at the branch level. From an FTC consumer protection perspective, it is important to note that we are not receiving complaints about inappropriate disclosure of bank records at this time.

Credit information

The Fair Credit Reporting Act[5] (FCRA) regulates the use of credit information by credit reporting agencies. Congress enacted the FCRA in 1970, and delegated primary enforcement responsibility to the FTC. The Fair Credit Reporting Act requires consumer reporting agencies to adopt strict procedures for providing information to credit grantors, insurers, employers and others. The Act permits credit bureaux to report only information that is timely and accurate. Credit bureaux may only disclose such information for a permissible purpose relating to credit, insurance, employment, and other transactions that consumers enter into primarily for personal, household, or family purposes. The Act also gives consumers certain notice, disclosure and due process protections. The FCRA limits government access to name, address and employment information from credit reports without a court order.

The FCRA is an important piece of privacy protection and has been shown to work well. It may, however, no longer make sense to limit its applicability to credit bureaux in this highly networked age.

Profiling and marketing

Widespread use and availability of computer generated records have increased concern about use of consumer information for profiling and marketing purposes. For example, the Video Privacy Protection Act[6] limits the circumstances under which disclosure of consumer video rental information may be made to the government and to the private sector. The Cable Communications Policy Act[7] requires the government to possess a court order to access cable records. Cable companies may distribute these records to third parties if they have notified consumers of their intention to do so, and consumers are permitted to prohibit its proposed re-use.

Conclusions

The US Government could facilitate the development of a privacy market in three distinct ways.

1. Government data should follow NIITF principles

The government should get its own house in order by ensuring that government data collection remains consistent with the NIITF Privacy Principles in the face of changing technology. The Office of Management and Budget (OMB) is responsible for enforcing the Privacy Act, for example, and might profitably review that statute along with federal agency adherence to it in the light of the NIITF Privacy Principles. OMB could report its findings and recommend legislation, regulation or executive orders to solve any problems it discovers. This kind of review could provide a model for the private sector to undertake similar audits.

2. Government could raise awareness of privacy

Government could play an important role in consumer and business education and, to some extent, this is already happening. The government could use agencies with responsibility for privacy as "bully pulpits" to raise consumer and business awareness of the issue. Consumer education is likely to raise demand for informational privacy protection to its optimal level. Business education is necessary to introduce technology entrepreneurs

4. Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 - 34 (1996).
5. Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 et seq. (1996).
6. Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1996).
7. Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1996).

to consumer protection theory, which in turn could help industry anticipate the privacy implications of a new product. The expense of consumer and business education would be minimised if the industries that will benefit most directly from increased consumer confidence in the GII were to accept some responsibility for this programme.

3. Government could appraise enforcement
Government could enhance self-regulation by exploring enforcement deficiencies with industry. This would address the most often-heard complaint about self-regulation: that industry codes of conduct are praiseworthy but unenforceable. Industry representatives often respond that competition law in the US limits their enforcement efforts. More work is needed to understand whether, and how, other values, including competition, undermine enforcement activities. Government and industry might then work together to resolve any such conflicts pro-competitively.

A competitive market for privacy may develop
One of the conclusions we can draw from the excellent response among industry and privacy advocates to the privacy workshop is that consumer privacy on-line is very much on everyone's mind. It is highly possible that in the on-line world, privacy may become a market commodity, given adequate levels of government initiatives and public education. As the number of transactions and services increase on the GII, consumer demand for privacy protections could continue to rise and a robust, competitive marketplace for privacy protection may very well develop. Under this scenario, the market itself could serve the same function as a privacy entity.

Christine Varney is a US Federal Trade Commissioner and former Cabinet Secretary to President Bill Clinton. The views expressed are those of the Commissioner and do not necessarily reflect the views of the FTC or any other individual Commissioner or staff.

This report is an edited extract from Christine Varney's presentation to the *Privacy Laws & Business* 9th Annual Conference in Cambridge, July, 1996. The rest of her paper and a detailed appendix of *Current and Pending Legislation on Privacy Rights and Technology,* prepared by her office, will be available from *Privacy Laws & Business* as part of the conference papers.