Inside the Beltway: The Politics of Privacy

Marc Rotenberg

As public concern about privacy grows, the Clinton administration and various trade groups in Washington, DC continue to sing "Don't worry, be happy," but a better song for government officials working the privacy issue might be that country western hit "You can't roller skate in a buffalo herd."

The administration has developed several sets of voluntary standards for privacy protection—each one drafted with the approval of industry, and each one completely unenforceable. It is a strategy intended to avoid real safeguards for consumers and serious inquiry into industry practices. Not surprisingly, consumer organizations, civil liberties groups and privacy advocates have given the White House low marks on the privacy issue.

> **The administration has developed several sets of voluntary standards for privacy protection.... It is a strategy intended to avoid real safeguards for consumers and serious inquiry into industry practices.**

First, came the draft code developed by the Office of Management and Budget (OMB). That initial draft moved privacy policy sharply from consumer protection to industry accommodation. The key twist was the treatment of the Code of Fair Information Practice—a generic term for privacy codes of conduct that have been part of information practices for more than twenty years. The codes had always placed responsibilities on data collectors, such as business and government, to protect privacy and given individuals rights of access and correction.

But the new OMB privacy code turned the tables. Now, the responsibility falls on consumers to find out about abusive record-keeping practices and the misuse of personal data. This approach is sharply at odds with standards that would restrict the misuse of personal data or provide legal incentives to pursue claims.

Then the National Information Infrastructure Advisory Council (NIIAC) and the National Telecommunication and Information Administration (NTIA) entered the picture. Instead of simply rejecting the initial OMB draft, as consumers organizations and privacy groups had urged, both the the NIIAC and the NTIA continued the charade, each group in turn recommending is own non-enforceable code of practice, and each code placing more burdens on consumers and users of new on-lines services and fewer responsibilities on companies and organizations that collect personal data. Both the NIIAC and the NTIA proposals emphasized notice provisions which allow organizations to avoid privacy safeguards by simply announcing "no privacy." Apply that regulatory approach to most consumer products and the risk to public safety would skyrocket overnight.

The NTIA also ignored calls to investigate industry practices, to explore options pursued in other countries, or even to examine the question of enforcement for whatever standards may be adopted. The NTIA approach is in sharp contrast to the outcome with similar agencies in other countries, such as the Ministry of Post and Telecommunications in Japan or the Canadian Standards Association, which have both pushed for enforceable legal rights for new online services.

The last act in what is clearly becoming bad drama came recently when the Federal Trade Commission announced that it too would pursue a voluntary code of

Caller ID

conduct to protect privacy. Even as the national papers ran front-pages stories about the $600 billion direct marketing industry acting without accountability, FTC commissioners said sincerely that the Commission would pursue voluntary standards until they were shown not to work. During the hearings, representatives of industry and direct marketing smiled as they have throughout this process, knowing that without enforceable legal rights consumers will have little opportunity to press privacy claims in the information age.

Just to be clear, there is no question that the White House can act with force in the privacy arena when it chooses to do so. It simply acts in the wrong way. The Clinton administration tried to push forward the Clipper encryption scheme until it ran into the brick wall that is the Internet user community and its fierce devotion to privacy. It did manage, with the help of some embarrassing lobbying, to push a wiretap bill to require the extension of surveillance to new communications technologies. But the cost of the proposal is so great and the implementation of the measure so impractical, that the prospects for going forward with the national wiretap plan, fortunately, continue to fade.

But if Washington continues to fumble the privacy issue, the same cannot be said for much of the rest of the country and for many other nations that have moved aggressively on the privacy front.

This past year the Europeans adopted a comprehensive privacy directive to protect the flow of personal information within the European Union. Although the US direct marketing association and its allies lobbied against the measure, a firm structure for data protection is now in place. The implications for the United States are interesting. Since the US lacks complimentary safeguards in many sectors, some US companies may be unable to do business in Europe and European privacy officials may restrict the flow of personal data to the United States because of inadequate consumer protection. An interesting twist on the old NAFTA problem.

US companies may be unable to do business in Europe and European privacy officials may restrict the flow of personal data to the United States because of inadequate consumer protection. An interesting twist on the old NAFTA problem.

The Europeans are also pursuing technical solutions to privacy protection. David Chaum, a noted cryptographer, won Europe's highest award for technical achievement last month for the Digicash system, which is now being deployed for everything from on-line payments to highway toll systems. (Techniques for anonymous payment like Chaum's could be more widely available in the US if the White House changed its policies on data encryption.)

Canada has also made important strides in the past year. New legislation to protect the privacy of records held by commercial firms is under consideration in the provinces and at the federal level. Even the Canadian Direct Marketing Association has called for enforceable legal privacy rights, noting, not surprisingly, that without a clear legal framework in place, companies that want to protect consumer privacy will not be able to compete effectively with companies that do not. (In fact, America Online made a similar admission last year when it explained the sale of its customer database by saying that it could not otherwise compete with other online service providers).

The states are also making good progress on privacy issues, pursuing statutory protections for personal information, limitations on the misuses of the Social Security Number, and sharp controls on the Caller ID service. The last development is particularly interesting because Caller ID represents a textbook example of a new consumer service that collapses once the privacy implications are uncovered. A better mechanism in Washington for evaluating services like Caller ID could have produced an outcome more favorable to both consumers and telecommunication service providers.

So, the question could well be asked, why is Washington so out of touch on the privacy issue?

1. ***Privacy is a classic public interest issue.*** Support is widespread but thin. Opponents of privacy measures are counting on the difficulty in organizing the public to oppose egregious industry practices. But the recent furor on the Internet with Clipper and the FBI wiretap bill, and the growing opposition to the unregulated sale of personal data may change the politics of this issue dramatically.

2. ***Washington lobbyists are writing the scripts for government officials.*** Much of the material that is coming out of Washington today from administration officials is being spoon-fed by industry. It is hard to find an original statement or concern voiced by any officials at OMB, NTIA, or the FTC. The process contrasts sharply with the experience in other countries and also with the US's own experience with the development of the original Code of Fair Information Practices back in 1973. Then, there was no question that officials had a responsibility to protect the public interest and to call for sharp controls on bad practices by both industry and government.

3. ***The public and the press are still not fully aware of the practices in the direct marketing industry or the consequences for the development of the Internet if strong safeguards are not put in place.*** A recent CNN segment focused on the Donnelley corporation's sale of personal data on young children through a 900 telephone number service, but other practices in the industry are even more troubling. Personal data on young children is routinely sold. Couple this data with interactive television services, and marketers and advertisers will quickly know more about the preferences of children than will the children's own parents. That issue, as much as any other, is likely to lead to significant reforms in the industry.

Why is Washington so out of touch on the privacy issue?

Indeed, the prospects for comprehensive privacy reform are not so bleak. Polling data shows strong support for much tougher privacy safeguards. A recent Yankelovich survey found that 90% of consumers favored enforceable legal rights against companies that invade privacy. This matches a 1991 Time/CNN poll which found that 93% of the American public believed that companies should not sell data without express permission.

Support is growing also for the "opt-in" approach, which would give consumers more control over personal data but is vigorously opposed by the direct marketing industry. As USA Today said in a recent editorial "opt-in does not trample on anyone's rights. Consumers can still get their catalogs and other direct-mail pitches by checking a box or clicking a mouse. Companies can still get data for marketing by asking for it. It would cause some inconvenience for businesses, which face increased costs to persuade customers to give up their privacy. But who should bear the burden: the businesses that glean the profit or the consumers whose information is sold?"

In the same editorial, USA Today also faulted the voluntary approach championed by the White House saying that "while voluntary compliance might be preferable in an ideal world, it's not likely to work in the real world. The reality is that the absence of government prodding has resulted in too many companies doing too little to protect consumers' privacy rights." (October 24, 1995).

Even these polls and editorials do not reflect the level of concern on the Internet today. Web users feel strongly about privacy and are savvy political organizers. Privacy will simply become more politicized as time passes.

Still, Washington policy makers are hoping to avoid a confrontation with powerful industry groups on the privacy issue. But by ignoring public concern, the White House has placed itself squarely on the wrong side of the issue. And if their positions don't change soon, people may start singing "Thank God and Greyhound they're gone."

.....

Marc Rotenberg is director of the Electronic Privacy Information Center in Washington, D.C.

More information about privacy is available from the EPIC web site <http://www.epic.org>.