



BRIEF ANALYSIS

No. 359

For immediate release:

Friday, April 27, 2001

Personal Privacy in a Transparent Society

By Devon Herrick

A torrent of personal information about each of us is available now and experts agree that it will increasingly become available to others who want to use it. Society has become much more transparent due to the advent of inexpensive computer technology, storage devices and the Internet. This development has led to concerns about how this information might be used by employers, marketers, health insurers and others. Carefully crafted laws that promote clear disclosure (and enforcement) of privacy agreements can help people protect themselves without sacrificing freedom of speech.

Personal Profiles.

Most experts agree that personal information will increasingly become available to those who wish to use it. Attempts have already been made to compile databases with personalized profiles. For example:

■ Lotus Development

Corporation announced plans to produce *Lotus MarketPlace: Households*, a software package expected to revolutionize direct marketing by making available the names, addresses, demographics and prior purchase behavior of 120 million U.S. consumers.

■ Internet advertising firm Doubleclick.com acquired a database of consumer buying habits with plans to integrate it with their own Internet surfing-habits database. This would allow marketers to know which products a consumer is likely to purchase and where best to advertise to obtain business.

Despite their appeal to marketers, the firms involved in these ventures backed away from them after experi-

encing public relations problems. However, there will be more efforts in the future.

Benefits of Information Sharing. There are trade-offs between privacy and efficiency, however. Laws against collecting data would restrict information about products a person might wish to purchase. They would also make commerce less efficient by wasting resources on poorly designed advertising campaigns promoting products for which there is no market. Some benefits of information sharing include:

■ Marketers can use consumer information to design and produce only products responsive to consumers' interests.

■ Scientists can use data from thousands of cases to discover the causes of disease and find cures or treatments that would otherwise go unnoticed.

■ Law enforcement can use public databases to solve crimes and track down criminals who might otherwise remain anonymous.

Risks of Information Sharing. Using a technique called "data mining" on databases of consumer information, medical spend-

ing histories and Web surfing habits, analysts are able to create personalized profiles on people. They can use this knowledge to make better predictions about life expectancy, health status, work habits and the like. However desirable use of these data appears to some, the resulting loss of privacy may be harmful to the individual. For example:

■ Life insurance companies might evaluate potential customers based on things such as speeding tickets that may not relate directly to longevity.

■ An individual might be branded as high-risk and charged more or denied health care coverage due to factors unrelated to health status.

Balancing Privacy and Free Speech

- Don't restrict First Amendment rights.
- Don't ban the collecting of consumer data
- Don't give individuals a property right in data about themselves.
- Allow consumers to opt out of data collection.
- Require clear disclosure of privacy policies.
- Facilitate agreements between affected parties.
- Monitor abuse and allow for remedies.
- Use contract law to enforce privacy agreements.

- An employer's evaluation of an applicant might be based partially on lifestyle as revealed by consumer preferences — such as money paid to a health club or purchases of liquor at a sports bar — rather than education, work history and ability.
- A potential mate might look at the individual's purchasing history, financial status and Web surfing habits before agreeing to a date.

The privacy of medical records has been protected to varying degrees for years. But the advent of the Internet has not only made more information of every kind more accessible, but has also made it accessible at less cost. Thus it's financially feasible for a health insurer to obtain in-depth personal profiles on potential customers. Because of this, many advocates have called for laws to protect the privacy of consumer information from those who may seek to use it. This is a complex issue, however. Possible solutions come with risks and may have adverse effects or unintended consequences.

Communication Privacy Protections. It is perfectly legal for a store, Web site or insurance company to collect information about you. There are a very few areas where communication is privileged and subject to extraordinary protections within the law: husband-wife, client-attorney, doctor-patient and priest-confessor. These are unique because the spouse or the advising party is under a legal and moral obligation to hold all communication in confidence. However, most other areas of communication are not protected from disclosure by either of the parties. Until recently this mattered very little. What protected us from excessive breach of privacy by third parties was the cost of gathering information. Someone wanting to delve into our personal, medical and financial history could do so only at a fair amount of expense. This is no longer the case.

Balancing Privacy and Free Speech. Purchases we have made, Web sites we have surfed or publicly available records such as driver's licenses, birth certificates, marriage records, etc., can contribute ultimately to breaching one's privacy. With the advent of the Information Age, many people advocate the creation of new laws to protect our privacy. Some would make it illegal to transfer information learned in the course of a two-party transaction to third parties. Others have suggested we should own a property right to all information about us. There are problems with these, however. Most attempts

to protect privacy restrict freedom of speech. A law restricting the ability to communicate facts about a person (such as lifestyle preferences or consumer purchases) would also restrict the press's freedom to report facts about newsworthy individuals.

There are also problems relating to the assignment of ownership of personal data. A copyright protects individual expression, but it is difficult to assign a property right to data such as your specific consumer habits. Some experts argue there is already a property right — and it is held by the collector of data. Besides, the Constitution does not guarantee a right to privacy whereas it does guarantee a right to free speech.

Rather than partially restricting our right to free speech, Congress should focus on ways to lower the cost of bargaining between affected parties. Contract law can be a mechanism for agreeing on and enforcing privacy policies. For example, marketers might be free to collect data but might have to disclose what is being collected and how it would be used. Retailers might be compelled to allow buyers the ability to opt out or to clearly advertise that they sell data, and risk losing the sale. Alternatively, sellers that collect and use data might agree never to transfer the information to a third party in return for a consumer's continued patronage. Organizations such as employers or insurance companies that rely on a third party for personalized data might be required to disclose the source upon request. Suppliers of personalized data might have to post policies on how to view and correct inaccuracies. Contract (or tort) law would enforce agreements.

Conclusion. There are no easy solutions to protect the privacy of consumer information from those wishing to profit from its use. There are, however, risks to our constitutional rights from formulating bad policy that restricts speech. Policy should follow Nobel Prize-winning economist Ronald Coase's theorem: make it easy to negotiate, specify each party's rights and allow the affected parties to bargain. Laws should promote clear disclosure of privacy policies, facilitate proper use agreements, allow individuals to monitor abuse and enforce the privacy agreements. This would allow people some control over whom they allow to learn facts about them and how those facts are used.

Devon M. Herrick is Research Manager for the National Center for Policy Analysis.

Note: Nothing written here should be construed as necessarily reflecting the views of the National Center for Policy Analysis or as an attempt to aid or hinder the passage of any legislation.

The NCPA is a 501(c)(3) nonprofit public policy organization. We depend entirely on the financial support of individuals, corporations and foundations that believe in private sector solutions to public policy problems. You can contribute to our effort by mailing your donation to our Dallas headquarters or logging on to our website at www.ncpa.org and clicking "An Invitation to Support Us."