18. Privacy and Private-Sector Databases

Congress should

- recognize the benefits for consumers of leaving the flow of new forms of information through the economy unrestrained;
- recognize the harm done to small business, new product development, and nonprofits by restricting the use of lists containing information about business customers; and
- respect the free flow of information between businesses about real events and real people.

Should private companies be allowed to keep information about their customers' buying habits and share that information with other businesses? There is growing tension between privacy alarmists' calls for regulation of the use of customer information by private-sector businesses and the free flow of information. From Al Gore's ''Electronic Bill of Rights'' to the Federal Trade Commission's threats of regulatory actions, privacy may become the regulatory foot in the door of the Internet.

Understanding the controversy over privacy will be critical throughout 1999, as the European Union has demanded that U.S. companies comply by October 1998 with privacy rules comparable to those the EU has adopted. Firms that fail to do so may find themselves barred from serving European customers. U.S. lawmakers should not allow Europeans to foist their confused privacy regulations on citizens of the United States, for the European model does little but empower new bureaucracies to restrict freedom.

Privacy: The New Censorship

Our freedoms have always included the right of human beings to learn about one another. Every day, each of us takes in an enormous amount

of information about people we encounter—their age and appearance, their manner of speaking and dressing, and their actions and preferences. Usually, we feel no obligation to ask anyone's permission before relaying the information we have collected to a third party, however embarrassing that might be to the subject of the conversation (''Did you notice that Bob Jones's suit was absolutely covered with dog hair?'').

People can use law, custom, and technology to create islands of privacy for themselves. Custom defines a doctor's obligation to protect his patients' privacy. But no law, contract, or custom stops the butcher from telling the grocer that Mrs. Jones has just bought a ham and might need some mustard. There is no reason that electronic commerce and databases maintained by private businesses should be treated differently.

Yet that is just what advocates of new privacy regulations propose. Many support the concept of ''mandatory opt-in.'' Here's how it works: Imagine you are starting a business that sells baby clothes in competition with a well-established department store. Under mandatory opt-in, you would not be allowed to buy a list of potential customers unless every single customer on the list had consented to that particular use of his name. Chances are, your business would not get off the ground.

Mandatory opt-in amounts to a restraint of information. If Sam buys a lawn mower from a hardware store, there are two parties to the transaction, Sam and the hardware store. It makes no more sense to let Sam prevent the store from giving out his name and address in a list of lawn-mower buyers than it would to give the store the right to forbid Sam to tell *Consumer Reports* what he thinks of the mower.

The mandatory opt-in rule would especially harm new ventures, from magazines to humane societies. New businesses absolutely depend on renting lists of customer information to compete with established competitors. *The brunt of an opt-in law would thus be borne by small, new businesses or nonprofits struggling to establish a customer base*.

Under mandatory opt-in, firms that could afford to send direct mail would no longer be able to target it effectively. That would lead to fewer, more expensive options for those who shop at home—the elderly, the disabled, rural residents, and anyone without a car—because their mobility is restricted. In a world without readily available, cheap marketing lists, it is doubtful that another company like Lands' End would ever be born.

No country that takes freedom of information seriously should prohibit a business from communicating information about real events and real people to other businesses. Attempts to restrict the transfer of information

run headlong into our right to free speech. New proposals to regulate it in the name of privacy are the latest kind of censorship.

The Uses of Information in the Economy

As more commerce moves on-line, the free flow of information becomes more vital to the economy. Traditional stores and new Internet retail outlets alike can capture enormous benefits by making the best use of information about their customers. As more exchanges than ever take place between distant strangers over electronic networks, businesses will no longer be able to rely on the personal knowledge of neighbors and regular customers to tailor goods and services to particular tastes. Gossip will give way to electronic libraries as the best source of consumer information.

Consumers will benefit, too, when producers and sellers can tailor their messages. Marketing to masses of uninterested people is expensive and wasteful. Targeted marketing, in contrast, puts information about new products and services into the hands of the consumers to whom it is most useful. New firms and products spring into existence, using new understanding of consumers' preferences to identify new market niches. Web sites that have tried to fund their operations by asking for subscriptions have seen drastic losses in their revenues and viewership. Likewise, advertisers have been disappointed by very low response rates (about 1 percent) to banner ads, which jeopardizes that source of revenue for Web sites. The sale of targeted advertising spots might provide a sounder foundation for electronic commerce.

Those who compile information in commercial databases have an incentive to keep the information accurate. The rates of significant errors in credit reports, for example, are low; a study of 15,703 consumers conducted by Arthur Anderson & Co. shows that the error rate is probably as low as 1 percent (other studies reporting higher rates of error made fundamental methodological errors and have been discredited).

Companies generally protect information about their customers from widespread disclosure to save their investment from competitors. Companies selling the use of their lists to direct marketers usually do so through third-party ''fulfillment houses.'' The company uses customer information to generate a list, then sends the list to the fulfillment house. The fulfillment house labels the mail to be sent out; the marketer does not even see the list or the labels, let alone the information in the files. To preserve its reputation, the fulfillment house must protect the company's list from disclosure.

In the new world of automated commerce, more formal electronic networks will naturally replace casual conversation as a source of information for businesses. Economists have documented how formal networks for checking credit and assessing the reliability of goods grow out of informal networks. Dun & Bradstreet, which reports on the creditworthiness of businesses, originated with Lewis Tappan, who managed credit accounts in his brother's silk business and exchanged letters with 180 correspondents throughout the country about the creditworthiness of businesses in their communities. Forty years ago community-based nonprofit organizations handled consumer credit reporting, which is now handled by three nationwide for-profit firms.

The evolution of formal information networks such as consumer credit reporting has important benefits for the public as a whole. Even the poor or those who are not well-known in a given community may buy on credit. The existence of credit reports gives consumers a reason to make payments on time, which means that businesses can lower the losses they suffer from default.

The formalization of the collection of information about consumers portends nothing sinister. Databases are a natural entrepreneurial adaptation to a more urban world, freed of small-town gossip.

Privacy and Children

The FTC and Vice President Al Gore have emphasized the importance of protecting children from Web sites that collect information from them on-line (note that, as of this writing, the White House for Kids Web site asks children for their names, ages, schools, and addresses—without any indication that parental permission is required).

In reality, children and their parents have little to fear from commercial sites; the sites' purpose is simply to sell more goods or services, hardly a sinister activity. The main risk seems to be that children might end up with a little more useless junk than they would have otherwise. Over time, children might—or might not—learn some valuable lessons from careless consumerism. Many children have been inexpensively educated about the pitfalls of mail order by the ''Sea Monkeys'' sold in comic books: to children's surprise, brine shrimp do not develop much personality or wear clothing, as the ads suggest.

Certainly, it would be possible for someone to abuse marketing information about children to do sinister things. Such abuse is real and not a trivial matter. But the risk is very small, especially compared with the

risks posed by information readily available in phone books and newspapers. In one infamous case, an imprisoned pedophile used stories about children cut from small-town newspapers to compile a list of 300 potential victims. Mailing lists invite abuse no more than do Internet chat rooms, noncommercial Web sites, newspapers, phone books—perhaps much less, because access to newspapers and phone books is cheap or free.

As it does for other media or on a public playground, the responsibility for ensuring a child's safety on-line should rest with the child's parents. Software is available that prevents children from giving out their names or addresses on-line.

A Constitutional Perspective on Privacy

The free-market view of privacy is that businesses should be free to trade with other businesses information they have gathered about their customers, as long as they have not agreed to keep it private. But what about privacy rights guaranteed by the U.S. Constitution? The answer to that is easy—the Constitution defines and limits the powers of the federal government, not the powers of private companies.

Government databases pose a serious threat that private databases do not for one fundamental reason: government alone may control the police, the armed forces, and the courts. Marketing agencies compile lists mainly to sell us things—a nuisance, but little more than that. We can protect our privacy from private marketers by limiting our use of credit cards. We hang up on telemarketers who call during dinner. But we dare not do that to the Internal Revenue Service.

Threats to privacy posed by government were the fundamental reason the Europeans adopted their version of privacy regulation, the data-protection laws. During World War II, the Nazis used government census data to track down Jews and other minorities. Similarly, in the United States census data were used to find Japanese-Americans and force them into camps. Europeans defend their model for protecting privacy, which tightly restricts government and business databases alike, by saying that they want to prevent the recurrence of such incidents.

But the Europeans have learned exactly the wrong lesson from history. It is wrong—and inherently inconsistent—to restrict private freedoms because of something government might do. We do not prohibit libraries from carrying *Mein Kampf* or *Das Kapital* on the theory that those works have been the inspiration of acts of violence and oppression on the part of the police. It makes no sense to stamp out direct marketing because

we fear government might seize the information and do harm with it. The threat would be better addressed by restrictions on the power of government.

The data-protection model seems more consistent with a deep, unfounded suspicion of information, business, and technology than with a real desire to limit the power of government. Note how the European data-protection model utterly fails to protect against government abuses of power or information. European data-protection laws are riddled with exceptions that favor government data collectors. Indeed, the premise of many European states seems to be that governments can be trusted with raw regulatory power over every aspect of citizens' lives, from medical care to education, and that a few trifling ''privacy'' rules can be trusted to prevent abuses. The resulting contradictions are Kafkaesque. Sweden, for example, adopted the first national data-protection model during the 1970s—at the same time the Swedish government adopted a sweeping system of national identification cards that Swedes today must show to write checks or use credit cards. While the French goverment is big on data-protection laws, citizens who want to work more than the allotted number of hours per week must work secretively out of their homes to evade labor inspectors.

The way to protect human rights around the world is to restrict the growth of government power. As the federal government becomes more entangled in the business of health care, for example, it demands greater access to medical records. As tax rates grow higher and the tax code more complex, the Internal Revenue Service claims more power to conduct intrusive audits and trace transactions. The Social Security system, now veering ever closer to bankruptcy, brought us problems with Social Security numbers. Health care legislation passed in 1996 created a new centralized medical database; the same year a law was passed requiring employers to register all new employees in a massive database. As our federal government grows, so will threats to privacy. Only holding back the power of government across the board will safeguard privacy—without any loss of Americans' freedom.

Recommended Reading

Klein, Daniel B. ''Why Consumer Opportunity Depends on Free Speech: The Credit Bureau as Social Accountability Mechanism.'' *Regulation*, forthcoming.

Klein, Daniel B., and Jason Richner. ''In Defense of the Credit Bureau,'' *Cato Journal* 12 (Fall 1992).

Singleton, Solveig. ''Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector.'' Cato Institute Policy Analysis no. 295, January 22, 1998.

—Prepared by Solveig Singleton