

17. Privacy and Private-Sector Databases

Congress should leave well enough alone and allow the market to address people's privacy concerns.

Because anything new is frightening, the growth of new information technology like the Internet provides a powerful emotional impetus for the creation of new privacy rights. Proposals to regulate the use of consumer information by private-sector companies have proliferated in the states and in Congress.

This “crisis” approach is a mistake. Seeking information about others is natural behavior. From businesses and finance institutions to shopkeepers, neighbors, coworkers, and friends, the normal rule of human relationships is that people are free to learn about other people and talk about them. Web sites are deaf and blind without the aid of cookies. Some professions—medicine and law, for example—require the assurance of confidentiality to gain their clients' trust. But freedom of information has been the rule, with laws protecting privacy the exception.

Privacy Regulation: An Extreme Approach

Proposals for regulation to protect privacy are more radical than their advocates realize. Many proposals would make it difficult for businesses to communicate facts about real people and real events to one another without satisfying elaborate notice and consent provisions. That turns the normal rule of freedom of information on its head. *This is an extremely radical idea with far-reaching consequences for consumers and the economy.* It is the legal equivalent of a sudden and massive expansion of copyright law, with a tremendous impact on information now in the shared domain. Consumers and constituents are unaware of the full consequences of adopting such extreme proposals.

Top Six Reasons Not to Impose Top-Down Privacy Regulation

- Calls for new privacy regulation are too extreme—like a drastic expansion of copyright law, proposed privacy laws would cut enormous quantities of information out of the shared domain.
- Small businesses, grassroots groups, political parties, and charities use information to get their foot in the door—privacy laws could shut them down.
- Consumers benefit from lower prices and enhanced competition when businesses use consumer information to cut the cost of offering new products.
- Consumers do not need the feds to step in to stop Safeway from knowing that they bought lettuce; there is no harm to consumers from legitimate businesses' use of information.
- Privacy regulation would hinder businesses from using advanced verification and tracing technology to fight fraud.
- Privacy legislation turning normal business practices on their head would throw U.S. businesses to the trial lawyers, creating an enormous liability risk.

Privacy Regulation Will Hurt Small Businesses, Grassroots Groups, and Political Speech

Consumers will always go to big companies with famous names, and big companies can afford to tangle with elaborate legal notices. But what about small businesses? Suppose you opened a store selling baby clothes in competition with JC Penney and Macy's. How would you find your first customers? Advertising by direct mail and on radio and television is very costly and has only about a 2 percent response rate. Even on the Internet, search engines are hit and miss—too risky for an entrepreneur to count on. The ability to buy a low-cost, updated list of families that have recently bought cribs in your area could mean the difference between success and failure for your small business. If you fail, that means less competition in the market, and that hurts consumers, too.

Privacy regulation that makes businesses face high liability risks or higher costs for processing information about consumers will naturally make lists shorter, less information-rich, and more expensive, as it has in Europe. Some lists may cease to exist entirely. This will have a potentially enormous impact on small businesses. Grassroots political groups, charit-

ies, and political parties also rely very heavily on the exchange of information to survive and grow.

Businesses' Use of Information Helps Consumers

Businesses use information about their customers for assessing credit risks, targeted marketing, just-in-time inventory control, product design, the customization of goods, improvements to customer service, and so on.

Economic studies of marketing reveal that ads are an important source of information about the features and price of new products for consumers. Those studies have found that the need to respond to competitors' marketing pitches forces each business to hold prices down and improve quality. Yet many Americans continue to believe that advertising and marketing make goods more expensive! That just goes to show that public opinion polls are not a good guide for policymaking.

Targeted marketing enhances the benefits of ordinary advertising, because it is less costly than mass mailings or random marketing. Using information to target marketing can lower the costs to a business for each sale from, for example, \$9.00 to \$2.00 per sale—and that means lower prices for consumers. Because of the use of information, consumers in the United States enjoy mortgage rates that on average are two percentage points lower than rates in the rest of the world.

If privacy regulation forces businesses to abandon targeted marketing, the high costs of nontargeted marketing will mean that some products are never offered to consumers at all. Meanwhile, big companies that can afford to deluge consumers with unwanted mailings will continue to do so.

Legitimate Businesses' Use of Information Does Not Harm Consumers

It is wrong to prevent businesses from exchanging truthful information about real people and events with others. Consumers do not need to be protected from businesses offering them goods and services. Broad privacy legislation merely strangles legitimate businesses in red tape, instead of focusing on fraud or real wrongdoing. Consumers may perceive the collection of information about them as vaguely scary, but that does not mean there is a real danger.

Privacy advocates view the collection of information about consumers as a harm in itself—an attack on human dignity or human rights. But that trivializes human dignity and human rights. Free-floating anxiety about

other people's knowing about us is hardly akin to torture or imprisonment. U.S. citizens do not need the federal government to step in to protect them because Safeway knows that they bought lettuce.

Privacy Regulation Would Hinder Fighting Fraud

Businesses are beginning to adopt new verification and authentication procedures to make sure they are dealing with the real person and not an imposter. For those procedures to work, businesses will need to collect, store, and process new types of personally identifiable information—and to have freedom to experiment. “Privacy-violating” technologies such as retinal scans, fingerprint-based verification systems, or sophisticated identity verification technologies are our greatest hope of *preventing* fraud. Thus there may often be a tradeoff between privacy and security. Consumers ultimately pay when businesses become victims of fraud. Privacy regulation that makes it hard for businesses to collect and exchange information about wrongdoers and trusted customers will get in the way of the battle against the real harm of fraud.

Identity theft and the use of information for fraud are real harms, but they are already illegal. The Identity Theft and Assumption Deterrence Act, passed in 1998, is beginning to work, although enforcement continues to be a challenge. New and more effective enforcement institutions that specialize in quickly resolving questions about true identity could be developed without more redundant laws.

Privacy Legislation Creates New Risk of Abuse by Trial Lawyers

The privacy legislation considered by Congress would give trial lawyers the opportunity to create a new class action nightmare for U.S. businesses. Enabling abusive class action suits by creating private rights of action for privacy violations is a bad idea. Class actions typically result in a trivial remedy for consumers, such as a bunch of coupons, while the lawyers that bring the case collect millions of dollars in fees.

Some businesses believe that federal legislation would reduce their risk of liability. That view is extremely naive. The privacy regulations proposed so far in Europe and the United States have been far too broad, vague, and counterintuitive to give reasonable guidance to the private sector. This is best illustrated by the concerns of small business in Britain about the

combination of baffling regulations and the threat of massive fines for noncompliance.

U.S. businesses have long operated in an atmosphere of freedom of information. They make a bafflingly complex variety of uses of information. The rapid pace of innovation will give rise to more baffling ethical and technical questions that centralized regulators are ill suited to judge. Insurance companies are reportedly unwilling to insure against such a liability risk, because the scope and nature of the threat of liability is so unclear. Congress would be wrong to make it impossible for U.S. businesses, especially small businesses, to insure against liability.

Conclusion: Time for a Reality Check

There is no simple answer to questions about privacy. The premise of privacy regulation has been that there is something horribly perverse about U.S. businesses, for they have not instantly responded to vague and changing regulatory demands for more and more privacy boilerplate. Is it really likely, though, that there is some sinister plot on the part of businesses to earn the distrust of their own consumers in a fiercely competitive market? The more likely answer is that strong advocates of regulation, who are isolated from the real world and the real economy, have started with artificial assumptions—and then become outraged because the world does not comply with their theoretical models. This failure of the regulatory advocates' understanding is then labeled a “market failure.”

The reality is that the question of privacy—when it is good, when it is bad—is far more complicated than would-be regulators have assumed. The economy as a whole makes uses of information too subtle and fast changing for central authorities to grasp. The privacy issue is an opportunity for legislators to show leadership and humility—to begin again by asking deeper questions and calling for real analysis instead of polling data.

Suggested Readings

- Calfee, John E. *Fear of Persuasion: A New Perspective on Advertising and Regulation*. Washington: AGORA Association and AEI Press, 1997.
- Klein, Daniel B., and Jason Richner. “In Defense of the Credit Bureau.” *Cato Journal* 12, no. 2 (Fall 1992).
- Klein, Daniel B., ed. *Reputation: Studies in the Voluntary Elicitation of Good Conduct*. Ann Arbor: University of Michigan Press, 1997.
- 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.

_____. “Privacy Issues in Federal Systems: A Constitutional Perspective.” Cato Institute Speeches, March 17, 1999, <http://www.cato.org/speeches/sp-ss031799.html>.

—*Prepared by Solveig Singleton*