

Protecting Privacy in the New Millennium: THE FALLACY OF "OPT-IN"

Executive Summary

Proponents of a radical new legal restriction argue that to protect privacy the government should prohibit the use of personal information unless consumers "opt-in" by giving their explicit consent for each and every use. On the contrary, a widely applied opt-in approach is simply bad public policy. "Opt-in" offers no greater privacy protection than allowing consumers to "opt-out" of uses of information to which they object, yet it imposes significantly higher costs on consumers, businesses, and the economy as it restricts the flow of information on which we all depend.

Information is the lifeblood of the U.S. economy. Legislators, regulators, and privacy advocates have been pushing vigorously for new limits on information flows in an effort to protect personal privacy. One of the most recent and severe of these restrictions has been the adoption of laws prohibiting the use of information unless the individual to which the information pertains "opts-in" to the use by giving explicit consent. These "opt-in" requirements replace the traditional standard of privacy protection in the United States, "opt-out," under which personal information about an individual may be freely used within defined legal limits as long as the individual does not "opt-out" of the use.

"Opt-in" is frequently portrayed as giving consumers greater privacy protection than "opt-out." In fact, the opposite is true. **"Opt-in" provides no greater privacy protection than "opt-out" but imposes significantly higher costs with dramatically different legal and economic implications.** Consider these critical distinctions:

1. **An "opt-in" system does not increase privacy protection.** "Opt-in" and "opt-out" both give consumers the final say about whether his or her information is used. Neither approach gives individuals greater or lesser rights than the other. Under either system, it is the customer alone who makes the final and binding determination about data use.

2. **An "opt-in" system is always more expensive than an "opt-out" system.** An "opt-out" system sets the default rule to "free information flow" and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an "opt-in" system sets the default rule to "no information flow," thereby denying to the economy the very lifeblood on which it depends. Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must rebuild the pipeline by contacting one customer at a time to gain their permission to use

information. "Opt-in" is more costly because it fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them.

3. Opportunities are lost under "Opt-In." By adopting a default rule that stops the free flow of information, "opt-in" impedes economic growth by raising the costs of providing services and consequently decreasing the range of products and services available to consumers. "Opt-in" would deny opportunities to consumers who now receive unsolicited material by phone or mail and have the option to act on those solicitations. "Opt-in" systems impose extra costs on everyone, *regardless of privacy sensitivity*, as compared to "opt-out" systems.

4. "Opt-In" reduces competition and raises prices. Switching from an "opt-out" system to an "opt-in" system would make it more difficult for new and often more innovative, firms and organizations to enter markets and compete. It would also make it more difficult for companies to authenticate customers and verify account balances, and thus frustrate the ability to counteract fraud. For both reasons, prices for many products would likely rise.

5. A move toward "opt-in" systems is contrary to consumer expectations. Opinion polls show that most consumers are happy to have their personal information used for appropriate purposes if they are given an opportunity to "opt-out." The behavior of 132 million adults who took advantage of direct marketing opportunities in 1998 backs up these polls.

6. "Opt-In" will increase the burden of unsolicited calls. By requiring an explicit statement of permission prior to use of personal information, an "opt-in" system necessarily requires businesses to make extra contacts with consumers. The extra burden on customers will increase again if the absence of personal information increases mass mailings and telephone calls because businesses can no longer target their marketing only to customers who are likely to be interested.

7. A broad application of "opt-in" rules may be unconstitutional. The use of "opt-in" requirements in situations where no clearly defined, significant harm is threatened may violate the First Amendment. The Supreme Court has declared unconstitutional many ordinances that would require affirmative consent, for example, before receiving door-to-door solicitations (*Martin v. Struthers*), before receiving Communist literature (*Lamont v. Postmaster General*), even before receiving "patently offensive" cable programming (*DAETC, Inc. v. FCC*). The U.S. Court of Appeals for the Tenth Circuit reached precisely the same conclusion in 1999, when the court struck down the Federal Communication's Commission's "opt-in" rule for the use of telephone subscriber information (*U.S. West, Inc. v. FCC*).

The conclusion is clear: **"Opt-in" is an exceptional tool that imposes high costs and harmful unintended consequences, and should therefore be reserved for exceptional situations where the risk of those costs and consequences is justified.**

Protecting Privacy in the New Millennium: THE FALLACY OF "OPT-IN"

By

Fred H. Cate¹
Michael E. Staten²

Proponents of a radical new legal restriction argue that to protect privacy the government should prohibit the use of personal information unless consumers "opt-in" by giving their explicit consent for each and every use. On the contrary, a widely applied opt-in approach is simply bad public policy. "Opt-in" offers no greater privacy protection than allowing consumers to "opt-out" of uses of information to which they object, yet it imposes significantly higher costs on consumers, businesses, and the economy as it restricts the flow of information on which we all depend

Free-flowing information is an essential component of the U.S. economy. Many of the characteristics of the "New Economy" (*e.g.*, just-in-time-delivery, total quality management, electronic commerce), and virtually all sectors experiencing strong growth, depend on the speedy, efficient availability of reliable information. So, too, do nearly all social and professional interactions. As many scholars have stressed: **"Information is the lifeblood that sustains political, social, and business decisions."**³

This is particularly true of financial information. As Comptroller of the Currency John Hawke, Jr., testified before Congress in 1999, our whole financial services sector is an "information-driven industry. . . . Information exchanges thus serve a useful and critical market function that benefits consumers and financial institutions alike, in facilitating credit, investment, insurance and other financial transactions."⁴

¹Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington.

²Distinguished Professor and Director of the Credit Research Center, The Robert Emmett McDonough School of Business, Georgetown University.

³Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 *Vanderbilt Law Review* 985, 987 (1983).

⁴Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of John D. Hawke, Jr.).

The Federal Reserve Board reached a similar conclusion in its 1997 report to Congress regarding consumers' personal financial information: "[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."⁵

Because virtually all of that essential information relates to individuals, legislators, regulators, and privacy advocates have been pushing vigorously for new limits on information flows in an effort to protect personal privacy. **Unfortunately, many of the proposed limits offer little by way of additional privacy protection but threaten to impose severe costs on the U.S. economy and impair the range and convenience of services that consumers enjoy and have come to expect.**

One of the most severe restrictions on information flows has been the adoption of laws prohibiting the use of information about an individual unless the individual "opts-in" to the use by expressing affirmative consent. These "opt-in" requirements replace the longstanding standard of privacy protection in the United States, "opt-out," under which personal information about an individual may be freely used within defined legal limits so long as the individual does not expressly prohibit such use ("opt-out"). Only in the narrowest of circumstances where privacy interests might legitimately thought to be at their highest (*e.g.*, certain uses of medical information⁶ or the use of credit reports for employment purposes⁷) is affirmative consumer consent required today for the use of personal information.

A recent and significant example of the legal shift toward "opt-in" was passage of the Shelby amendment to the Department of Transportation Appropriations Act in 1999.⁸ The amendment eliminates federal highway funds for states that do not require affirmative "opt-in" consent from individuals before information about them contained in driver's and motor vehicle records is used for marketing and survey purposes. The provision thus reverses the position that the Congress took on such records in 1994 in the Drivers' Privacy Protection Act, which allowed states to presume consent for the disclosure of nonsensitive information in public records unless an individual "opts-out."⁹

"Opt-in" is frequently portrayed as offering consumers greater privacy protection than "opt-out." In fact, the opposite is true: **"Opt-in" provides no greater privacy protection than "opt-out" but imposes significantly higher costs with dramatically different legal and economic implications.** Consider these critical distinctions:

⁵Board of Governors of the Federal Reserve System, Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2 (1997).

⁶15 U.S.C. § 1681b(g).

⁷Id. § 1681b(b).

⁸Department of Transportation and Related Agencies Appropriations Act, 2000, § 350, 106 Pub. L. No. 69; 113 Stat. 986 (1999).

⁹18 U.S.C. §§ 2721-2725.

1. Consumer Control over How Personal Information is Used. "Opt-in" and "opt-out" both give consumers the final say about whether his or her information is used. Neither approach gives individuals greater or lesser rights than the other. As a result, there is little difference in the privacy protection provided by "opt-in" and "opt-out" systems: under either system, it is the customer alone who makes the final and binding determination about data use. **Shifting from an "opt-out" system to an "opt-in" system does not increase privacy protection.**

2. Economic Cost. There is a stark difference between "opt-in" and "opt-out" in terms of cost. An "opt-out" system presumes that consumers **do want** the convenience, range of services, and lower costs that a free flow of personal information facilitates, and then allows people who are particularly concerned about privacy to block the use of their information. Put another way, the "opt-out" system sets the default rule to "free information flow" and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an "opt-in" system presumes that consumers **do not want** the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.

In other words, an "opt-in" system sets the default rule to "no information flow," thereby denying to the economy the very lifeblood on which it depends. Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must rebuild the pipeline by contacting one customer at a time to gain their permission to use information.

Consequently, an "opt-in" system for giving consumers control over information usage **is always more expensive than an "opt-out" system.** Opt-in requires that every consumer be contacted to gain explicit permission. Under opt-out, contact only occurs for those consumers who wish to withhold permission. Opt-in is more costly precisely because it fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them.

3. Opportunities Lost: The Consequences for Products and Services. By adopting a default rule that stops the free flow of information, "opt-in" impedes economic growth by raising the costs of providing services and consequently decreasing the range of products and services available to consumers. While individual consumers may "opt-out" of a specific information use without making the overall provision of services based on that use economically untenable, it is far more difficult to create and market new services based on building up a base of consumers who have decided, when contacted, to "opt-in" to the necessary information exchange.

To illustrate the cost of setting a default rule that halts the free flow of information, consider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system. In obtaining permission to utilize information about its customer's calling patterns (*e.g.*, volume of calls, time and duration of calls, etc.), the company found that an "opt-in" system was significantly more expensive to administer, costing almost \$30 per customer contacted. To gain permission to use such information for marketing, U.S. West determined that it required an average of 4.8 calls to each customer household

before they reached an adult who could grant consent. In one-third of households called, U.S. West *never reached the customer*, despite repeated attempts. Consequently, many U.S. West customers received *more calls* than in an "opt-out" system, and one-third of their customers were denied opportunities to receive information about valuable new products and services.¹⁰

An "opt-out" system allows individuals with privacy concerns to prohibit certain uses of their information, but it also permits people who are less concerned about the privacy of basic information, such as that used in most direct marketing, to learn about new services and products they might value. In an "opt-in" system, the privacy-sensitive group gets the same level of protection, but both they and those consumers less concerned about privacy lose many opportunities to take advantage of information-dependent services, whether instant credit, targeted marketing, unified frequent travel programs, or personal shoppers.

In short, "opt-in" systems impose extra costs on everyone, regardless of privacy-sensitivity, as compared to "opt-out" systems. Restrictions on information flows inevitably restrict the range of opportunities to which consumers will be given the chance to consent in the first place. Businesses incur higher costs of finding new customers because they must rely on mass advertising, mailings and telephone calls rather than targeting their marketing efforts at consumers who are likely to be interested. In addition, the lack of readily available personal information denies firms a key tool used to prevent and detect fraud, putting further upward pressure on costs, and ultimately prices.

4. Reduced Competition. "Opt-in" systems harm markets in other ways as well. Robert E. Litan, Director of the Economic Studies Program and Vice President of The Brookings Institution, and a former Deputy Assistant Attorney General for the United States, has written that switching from an "opt-out" system to an "opt-in" system would "raise barriers to entry by smaller, and often more innovative, firms and organizations," make it more difficult for "companies to authenticate customers and verify account balances, and thus frustrate the ability to counteract fraud," raise prices for many products and services "because competition would be reduced while fraud-related and marketing costs" would be higher, and deny opportunities to "consumers who now receive unsolicited material by phone or mail and act on those solicitations."¹¹

5. Consumer Expectations. One irony of the move to "opt-in" systems is that they are contrary to consumer expectations and behavior. The opinion polls that demonstrate that many consumers are increasingly concerned about their privacy also show that those same consumers are happy to have their personal information used for appropriate purposes so long as they are given an opportunity to

¹⁰Brief for Petitioner and Intervenors at 15-16, *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

¹¹Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, in Lucien Rapp and Fred H. Cate, *European and U.S. Perspectives on Information Privacy* (forthcoming).

"opt-out."¹² Demonstrated consumer behavior backs up these polls. For example, more than two-thirds of U.S. consumers—132 million adults—took advantage of direct marketing opportunities in 1998,¹³ accounting for more than \$1.3 trillion in sales of goods and services.¹⁴ Presumably one reason that direct marketing remains popular even as privacy awareness escalates is because the Direct Marketing Association provides a convenient way for consumers to "opt-out" of the use of their personal information by member companies. Over the past decade, however, fewer than 3 percent of U.S. adults availed themselves of that opportunity.¹⁵ The conclusion is inescapable: The vast majority of the public does not object to the reasonable use of information about them if they know that they *can* "opt-out" of such uses should they choose to.

6. Customer Burdens. By requiring an explicit statement of permission prior to use of personal information, an "opt-in" system necessarily requires businesses to make extra contacts with consumers to determine whether they wish to "opt-in," as compared with an "opt-out" system, under which consumers contact businesses if they do not want their information used. The burden on customers is increased further if the absence of personal information causes businesses to replace their more narrowly targeted messages with greater use of mass mailings and telephone calls. Since businesses lack the personal information necessary to identify which consumers are likely to be interested, their reliance on mass mailings to promote new products will mean that many consumers who have no interest whatsoever will receive "junk mail." In addition, customers face another risk, because the lack of personal information denies business a key tool used to prevent and detect fraud.

7. Constitutionality. The use of "opt-in" requirements in situations where no clearly defined, significant harm is threatened may very well violate the First Amendment. The Supreme Court has struck down many ordinances that would require affirmative consent before receiving door-to-door solicitations,¹⁶ before receiving Communist literature,¹⁷ even before receiving "patently offensive" cable programming.¹⁸ The words of the Court in the first case—involving a local ordinance that banned door-to-door solicitations without affirmative householder consent—are particularly apt:

¹²See, e.g., Personalized Marketing and Privacy on the Net: What Consumers Want, A Privacy & American Business Consumer Privacy Survey Questionnaire (Development and Report by Dr. Alan F. Westin, Fieldwork and Data Preparation by Opinion Research Corporation) (Nov. 1999).

¹³Direct Marketing Association, Economic Impact: U.S. Direct Marketing Today (4th ed.), 1998.

¹⁴Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of Richard A. Barton).

¹⁵Id.

¹⁶Martin v. Struthers, 319 U.S. 141 (1943).

¹⁷Lamont v. Postmaster General, 381 U.S. 301 (1965).

¹⁸Denver Area Educational Telecommunications Consortium, Inc. v. FCC, 518 U.S. 727 (1996).

Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household, and not upon the determination of the community. In the instant case, the City of Struthers, Ohio, has attempted to make this decision for all its inhabitants.¹⁹

The U.S. Court of Appeals for the Tenth Circuit reached precisely the same conclusion in 1999, when the court struck down the Federal Communication's Commissions "opt-in" rule for the use of telephone subscriber information.²⁰

Conclusion

"Opt-in" is an exceptional tool that imposes high costs as well as harmful, unintended consequences. It should be reserved for exceptional situations where the risk of those costs and consequences is justified. One example might be in the collection of data from children on the Internet. Another might be in the release of medical records for a variety of purposes. In most other settings, the higher costs imposed by an "opt-in" system are unwarranted; for this reason the United States has historically eschewed "opt-in" systems. Moreover, the indiscriminate use of "opt-in" means that this exceptional privacy protection will no longer signal that a particularly significant privacy interest is at risk.

This is the ironic lesson from Europe, where the 1995 EU data protection directive requires businesses and governments alike to obtain affirmative consent before collecting or using any personal information.²¹ Many observers wondered how the European economy would be impacted by such a broad application of the "opt-in" requirement when it took effect in 1998. But, to date, national data protection authorities have permitted data collectors and users to rely on "opt-out" for all but the most sensitive data. "Opt-in" may be the law on the books throughout Europe, but "opt-out" is the reality because government officials realize the blow that an "opt-in" requirement would deal to European economic performance.

In summary, legislators and policymakers should carefully consider the costs associated with an "opt-in" regime, especially since it accords consumers with no greater rights than an "opt-out" system. Those costs are measured not only in economic terms (higher prices and lost opportunities), but also in additional burdens on consumers and businesses alike, and infringement upon the open flow of information guaranteed in the First Amendment.

As the Tenth Circuit concluded:

¹⁹319 U.S. at 141.

²⁰U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

²¹Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data art. 25(1) (Eur. O.J. 95/L281).

Even assuming that telecommunications customers value the privacy of [information about their use of the telephone], the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. *Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.*²²

²²Id. (emphasis added).