Privacilla.org

Your Source for Privacy Policy from a Free-market, Pro-technology Perspective

Affiliate-Sharing and Consumers:

How "Privacy" Regulation Misses the Mark, Hits Marketing

A Special Report Issued by Privacilla.org
http://www.privacilla.org

November, 2003

Introduction

"Affiliate-sharing" is the latest buzzword in commercial privacy regulation. In the name of privacy, the bell-weather state of California has passed new law regulating the sharing of information among related corporate affiliates. Regulation of third-party sharing has become law there too.

The relationship between affiliate-sharing and consumer privacy has long been assumed and advocated for, but never deeply studied. Affiliate-sharing regulation may advance privacy for some set of consumers, but others — possibly a large majority — may get little benefit from it.

It is unwise to pass blanket privacy laws for the benefit of a few privacy outliers, but this may well be what has happened in California and what is threatened for the whole nation in current congressional debates.

Experience in the marketplace and with prior regulation suggests that affiliate-sharing is not a significant privacy concern for consumers. At least one financial services company has tried to use strong privacy protections to win customers and failed to succeed. Regulation that gives consumers the choice to opt-out of some commercial information-sharing has met with anemic responses — one-tenth the size of regulatory programs that promote a true consumer interest.

The lessons of experience reveal that:

- Effective privacy regulation focuses on preventing harms rather than establishing obscure consumer "rights" like prevention of affiliate-sharing.

- Consumers choose publicity as often as the choose privacy. It is wrong to assume that most or all consumers choose privacy over other interests.

- Many consumers dislike intrusive marketing, but more likely because of the intrusion than because of the marketing.

In the end, the debate about corporate information sharing, whether with affiliates or third parties, has more to do with marketing and marketing practices than with privacy protection. Though they are often related, marketing and privacy are vastly different issues.

With threats to privacy from government continuing to grow, the privacy issue is too important to be sidetracked as a debate about the convenience of commercial communications. Rather than calling anti-marketing proposals "privacy protection," advocates of regulation should openly call for restrictions on commerce and commercial speech. Then a debate on the role of commerce in the lives of American consumers could take place. Thanks to new law, the role of commerce in the lives of Californians is already under a very interesting cloud.

A Spate of Regulation Aimed at Commercial Information Practices

For a variety of reasons, most large enterprises today are not a single corporation, but multiple affiliated corporations. Tax laws, regulatory requirements, and corporate laws often force a large business to offer the variety of services it does through different, closely related corporations. This is true for many industries, but especially for financial services.

Each corporation in a family of affiliates is usually subject to common ownership and control, often under a single holding company. A corporate family will typically use the same brand, operate through the same channels of commerce, and share locations, computer systems, advertising budgets, and so on.

Breaking one enterprise into separate, affiliated corporations generally allows tax savings and efficient compliance with regulations. The savings can be passed on to consumers in the form of lower prices and to stockholders in the form of higher returns. Conducting multiple lines of business under one brand through affiliates delivers consumers one-stop shopping for the goods and services they want.

To expand customer relationships and generate additional revenue, businesses with corporate affiliates often share information among themselves. Personal information about customers is shared regularly among families of corporations. This is what the "affiliate sharing" debate is about. "Third-party sharing" is, of course, when information is shared with entities outside the corporate family.

As long as highly complex tax and regulatory schemes require businesses to have multiple affiliates, they should have them, for the savings and efficiency that corporate affiliation brings. The separateness of corporate affiliates certainly matters for tax and regulatory purposes, but it is an open question whether this matters to consumers. Sharing of information among affiliates may be an acute privacy concern, or consumers may recognize that the separateness of affiliates is meaningless for their purposes. Consumers may prioritize getting goods and services conveniently, at reasonable prices, from companies they trust.

In a truly unique political and legislative year, California has leapt out of the gate with legislation regulating affiliate sharing and the companies that practice it.

California Leaps to Regulate

In a truly unique political and legislative year, California has leapt out of the gate with legislation regulating affiliate sharing and the companies that practice it. This has accelerated a debate about affiliate sharing and privacy that deserves full exploration and discussion.

The California Financial Information Privacy Act[1] became law in late August 2003. Effective July 1, 2004, it requires financial institutions to allow consumers to refuse sharing of information about themselves with affiliates and affinity partners. The law specifies in detail the form that must be used to communicate about this with consumers. The law also prohibits financial institutions from sharing consumer information with third parties unless the consumer has given consent to the sharing. Another form is specified for this purpose.

A company that negligently violates the California Financial Information Privacy Act can be fined from $2,500 to $500,000 regardless of whether any consumer is harmed. A company that knowingly or willfully violates the law may be required to pay $2,500 per individual whose information was shared, again without respect to actual harm, and with no cap on the total penalty that may be paid.

A company that negligently violates the California Financial Information Privacy Act can be fined from $2,500 to $500,000 regardless of whether any consumer is harmed.

A second California law,[2] effective January 1, 2005, applies to all the businesses in the state that are not subject to the California Financial Information Privacy Act if they disclose customers' personal information to third parties for direct marketing purposes. The definition of third parties includes "separate legal entit[ies]," which assumedly includes both third parties and affiliates.

On request, these businesses must provide customers a list of the types of information that they share and the names and addresses of the entities with whom they share it. These businesses are also required to place links titled "Your Privacy Rights" on their home pages, and to provide information about the disclosure process on the linked pages. This law penalizes businesses $3,000 per violation for willful violations or $500 for ordinary violations, plus attorneys fees and costs, even though violations cause consumers no recognized harm.

Federal Preemption and Legislation

To the extent it regulates affiliate-sharing, the California Financial Information Privacy Act is preempted by the federal Fair Credit Reporting Act (FCRA).[3] In July of this year, a District Court in California reaffirmed that, under a key provision of the FCRA, states may not regulate information sharing among entities affiliated by common ownership or control.[4] The FCRA does not preempt regulation of third-party sharing.

[1] S.B. 1 <http://www.leginfo.ca.gov/pub/bill/sen/sb_0001-0050/sb_1_bill_20030828_chaptered.pdf>.
[2] S.B. 27 <http://www.leginfo.ca.gov/pub/bill/sen/sb_0001-0050/sb_27_bill_20030925_chaptered.html>.
[3] 15 U.S.C. § 1681 et seq. <http://www.ftc.gov/os/statutes/fcra.htm>.
[4] Order on Cross-Motions for Summary Judgment, Bank of America v. City of Daly City, No.s C 02-4343 CW; C 02-4943 (N.D.Cal. July 29, 2003).

The FCRA preemption provision stops having effect on the first day of January 2004. If Congress does not extend it or make it permanent, states will be able to pass laws in 2004 and beyond to regulate affiliate sharing.

Naturally, affiliate and third-party sharing has quickly become a hot topic in current congressional debate about the FCRA. Legislation in the House of Representatives would leave in place the national rule allowing affiliate sharing.[5] But the Senate version of the legislation would require special affiliate-sharing notices when the sharing is for marketing purposes.[6]

The Senate bill would require companies to allow consumers to forbid or limit the solicitations they receive based on such information sharing. An amendment that is likely to be considered when this legislation is debated on the Senate floor would require notice of all affiliate sharing to be given to consumers and a similar opportunity to forbid or limit the practice.[7]

In varying degrees, each of these laws, bills, and amendments have been described or touted as privacy protection. With affiliate-sharing regulation having such a prominent place in current debates, it is worthwhile to examine its actual effects on privacy — indeed, whether such regulation is "protection" from anything. And, of course, the level of interest real American consumers have in regulation of this sort should be gauged.

Understanding Privacy

The starting point for determining the role of affiliate sharing regulation in privacy protection is to solidly capture the concept of "privacy." The term is rarely defined before being used to advance one cause or another. This has served poorly the policy-makers who want to do right for their constituents. And it has harmed the people who must live with the laws and regulations that result.

Identity fraud has long been characterized as a "privacy" problem, for example, distracting lawmakers and law-enforcers from the fact that it is a crime for which people should be going to jail. Identity fraud rates have continued to grow and Americans have

[5] Fair and Accurate Credit Transactions Act of 2003, H.R. 2622, 108th Cong., 1st Sess. § 101 (2003).
[6] National Consumer Credit Reporting System Improvement Act of 2003, S. 1753, 108th Cong., 1st Sess. § 214 (2003).
[7] Both the Senate bill and the amendment would renumber a section of the Fair Credit Reporting Act that authorizes the Federal Bureau of Investigation to obtain citizens' financial information secretly using administrative subpoenas. 15 U.S.C. 1681u. Government snooping is a greater threat to privacy and other key interests than any data collection and use in the private sector. It seems ironic that language empowering federal agents to secretly tap the credit reporting system is moved aside to make way for regulation of affiliate sharing. Doing so is something like pulling the pin on a grenade for use as a toothpick.

suffered because of the persistent association of identity fraud and other crimes with "privacy."[8]

Defining Privacy

Privacilla.org has formulated a definition of "privacy" that describes the concept and allows other concepts to be distinguished. Privacy is a state of affairs individuals experience having to do with the amount of personal information about them that is known to others and on what terms. Specifically, *privacy is the subjective condition that people experience when they have power to control information about themselves and when they have exercised that power consistent with their interests and values.*

A Subjective Condition

"Privacy" is rarely defined before being used to advance one cause or another.

Foremost, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be. Likewise, government regulation aimed to deliver privacy is likely only to create confidentiality or secrecy rules based on the guesses of politicians and bureaucrats about what consumers' sense of "privacy" might be. Such rules can only crudely ape the privacy-protecting decisions that millions of consumers would otherwise make in billions of actions, transactions, and inactions every day.

The Role of Law

An important factor in the definition of privacy — power to control information — essentially goes to the influence of law. Law determines whether people are empowered to protect privacy. It has dual, conflicting effects.

On one hand, law protects the privacy-enhancing decisions people make. By enforcing contracts, protecting bodily integrity and property rights, and so on, law reinforces the privacy-protecting decisions consumers make. A body of U.S. state tort law also directly protects privacy, giving anyone in the possession of sensitive personal information the responsibility to protect it and use it tactfully, if at all.[9]

On the other hand, law often undermines individuals' power to control information. There are three major ways that law and regulation does this.

Some laws can be characterized as "anti-privacy." These prevent consumers from using privacy-protecting technologies or practices, or they prevent businesses and consumers from agreeing to control what is done with personal information. The Bank Secrecy Act is a good example. It requires financial institutions to report consumer

[8] *See* Understanding Amy Boyer's Law: *Social Security Numbers, Crime Control, and Privacy,* Privacilla.org (December 2000) <http://www.privacilla.org/releases/AmyBoyer.html>.

[9] *See* The Privacy Torts: *How U.S. State Law Quietly Leads the Way in Privacy Protection*, Privacilla.org (July, 2002) < http://www.privacilla.org/releases/Torts_Report.html>.

information to the U.S. government for entry into a law enforcement database. Under this law, even perfectly law-abiding citizens can not arrange to keep their financial affairs private.

Government surveillance programs are a second way that law rends control of information from people. Surveillance is collection of information undertaken without the consent or participation of citizens, often contrary to their efforts to conceal it.

The third major way that law and government programs deprive people of power to control information is through the creation of public records — and particularly public records databases. When information is in government hands, individual citizens may no longer control what happens with it. And when it is in electronic form, information is uniquely persistent, transferable, copyable, and usable. Many entitlement and tax programs show how the helping hand of government strips away privacy before it goes to work.

The Role of Choice

Perhaps the most important, but elusive, part of privacy protection is consumers' exercise of power over information about themselves consistent with their interests and values. This element requires consumers and citizens to be aware of the effects their behavior will have on their privacy, and to act accordingly.

Technology and the world of commerce are rapidly changing, and personal information is both ubiquitous and mercurial. This makes relationships between personal information, behavior, and privacy difficult to catalog, even for full-time students of information policy.

An active advocate community, a watchdog press, and a variety of government bodies are constantly educating the public and looking for privacy violations. Their work advances market solutions.

Though it may be difficult to exercise, consumers in a free market always have the power and choice to absent themselves from privacy-invading transactions. To help them, there is an active advocate community, a watchdog press, and a variety of government bodies that are constantly educating the public and looking for privacy violations.

Many of these institutions are also seeking to impose their privacy preferences rather than letting consumers decide, but much of their work advances market solutions all the same. Relying on consumers to pursue privacy and all their interests in the marketplace is the best way yet devised to get consumers precisely what they want.

Privacy is delivered when people have the power to control information about themselves and when they use that power in ways they want. Americans make a wide variety of choices about personal information. Some affirmatively seek publicity for information about themselves that others view as gravely personal. There are examples

throughout society, in the different ways that people treat their religious thinking or political views, for example, or the different treatments they give to information about relationships, family, or health. Our assumptions and the conventional wisdom about privacy are as often wrong as they are right.

Affiliate-Sharing Regulation and Privacy

Comparing affiliate-sharing regulation to a well-defined conception of privacy reveals that it has to do with privacy in only a limited sense. To reach this conclusion, we take the key elements of the privacy definition above.

Subjective Condition

Though advocates constantly generalize, consumers' subjective feelings about affiliate-sharing probably vary widely. Some may find it deeply offensive. Some may think it is the greatest innovation financial services ever enjoyed. Many probably lie in between, and many others have probably never considered it. Consumers are entitled to have no opinion at all on certain business practices and it is rational to ignore practices that are non-harmful or trivially harmful.

It is unknown whether the great bulk of consumers believe affiliate-sharing is a privacy concern. Privacy surveys have been debunked as a tool for learning actual consumer interests.[10] The best available evidence is consumer behavior, which should reflect consumers' interests and priorities best. Some advocates and lawmakers, of course, believe that market processes have not revealed or can not reveal latent consumer demand.

Power to Control Information

Affiliate-sharing regulation does not strengthen or weaken the legal power consumers have to control information about themselves. Consumers who object to affiliate sharing already have all the power they need to address it. They can and do refuse business with financial services conglomerates.

Consumers who object to affiliate sharing already have all the power they need to address it. They can and do refuse business with financial services conglomerates.

In 2002, the U.S. Senate Banking Committee estimated that as much as 10% of the nation's households are "unbanked," meaning that they do not have a bank account at an insured depositary institution.[11] For the majority, largely poor and immigrant communities, this has accurately been ascribed to limited financial sophistication. But a small portion of the "unbanked" are financially literate and have chosen to stay out of the financial services sector because of its high costs in privacy. This may be because of

[10] *See* With a Grain of Salt: *What Privacy Surveys Don't Tell Us*, by Solveig Singleton and Jim Harper, Competitive Enterprise Institute (June 1, 2001) <http://www.cei.org/gencon/025,02061.cfm>.
[11] U.S. Senate Committee on Banking, Housing, and Urban Affairs, *Sarbanes Announces Hearing on the "Unbanked"*, (April 25, 2002) <http://www.senate.gov/~banking/prel02/0425unbk.htm>.

affiliate sharing, because government access to personal financial information is increasing, or for some other privacy-related reason.

The power to decline transactions is an enormous, if unseen, force in the marketplace. It chastens companies to constantly seek better ways to serve consumers. If consumers do not want to do business, out of privacy concern or for any other reason, nobody is going to stop them.[12]

There should be no mistaking that exercising the power of exit can be expensive. This is a testament to the highly developed financial services and commercial system we have in the United States. This system makes transactions fast, inexpensive, and convenient for participants. And it will accommodate the needs of consumers who have privacy concerns, if a large enough group of them exist to be served as a niche market.

The outliers, consumers who decline to take part in the financial services system because of irrational or anomalous privacy concerns, are in the same position as consumers who refuse to ride in buses or automobiles because of safety concerns. They can expect a difficult time enjoying a life similar in ease and luxury to other consumers.

Exercise of Control

Perhaps, however, affiliate-sharing regulation can help consumers tailor their use of the power to control personal information.

Perhaps affiliate-sharing regulation can help consumers tailor their use of the power to control personal information.

Some forms of affiliate-sharing regulation may allow some consumers to exercise more precise control over how information about themselves is used within financial services providers and other businesses. Other forms may improve consumers' knowledge that affiliate sharing occurs, so they may develop rational privacy-related concerns about it. Some consumers may have existing concerns, but find themselves frustrated when they attempt to learn good information about the information practices of companies with which they do business. And, certainly, individuals or small numbers of consumers have had little ability to bargain with nationwide or global companies for precise control over affiliate-sharing. In this sense, affiliate-sharing regulation may represent a marginal improvement in the privacy of consumers.

There is an equally plausible case that affiliate-sharing regulation deprives consumers of control, or at least deprives them of the benefits of control. One exercise of control is to let personal information be shared and put to its highest and best use in lawful commerce. This redounds to consumers' benefit in the form of tailored customer service, better products, and lower costs.

[12] With apologies to Yogi Berra: "If people don't want to come out to the ball park, nobody's going to stop them."

Because the costs and lost efficiencies from affiliate-sharing regulation will fall on all consumers, those who would allow personal information to be shared will pay higher prices or forgo services and innovations along with the rest. If a large majority of consumers do not regard affiliate-sharing as an action-worthy privacy concern, a high price is paid by the majority so that a small group of privacy zealots can be satisfied.

Thus, the question is posed: Will affiliate-sharing regulation serve the mass of consumers, or impose heavy costs on the majority of consumers for the benefit of a few privacy outliers?

Affiliate-Sharing Regulation: Costs to Many, Benefits to Few

There is some evidence about affiliate-sharing and privacy from real world experience. It suggests that affiliate-sharing is probably not an actionable priority for most consumers. Accordingly, affiliate-sharing regulation probably imposes disproportionate costs on the majority of consumers to serve the privacy interests of a small minority. This evidence comes from both the marketplace and experience with regulation.

The Marketplace Experience

Time and again, entrepreneurs who believe they understand consumer desires throw investment and effort after their beliefs. They seek handsome rewards if they are right, knowing that they will be socked with losses if they are wrong.

Affiliate-sharing regulation probably imposes disproportionate costs on the majority of consumers to serve the privacy interests of a small minority.

More often than they succeed, business models and companies fail to assemble products, practices, and protections that please consumers. They disappear unannounced and unnoticed. Watching success and failure among businesses provides some indication of what consumers look for.

The experience of one California business provides evidence that financial privacy is not a high action-item for consumers and suggests that consumers are relatively satisfied with existing information practices. This business case comes with an interesting twist.

ELoan.com is an online financial services firm that has tried for several years to get traction with a business model that claims high protections for privacy. Evidently, other qualities in financial services providers are a priority to consumers. ELoan.com's information practices have not distinguished the company in a way that appeals strongly to consumers, so growth has been slow.

Unfortunately, eLoan's CEO has blamed the problems of his company on overall distrust of the financial services industry so — here is the twist — he funneled more than a million dollars into signature-gathering for a financial privacy initiative in California. When it was clear that he had purchased enough signatures to place the initiative on the ballot, he cut a deal with some of the state's large financial services providers allowing the California Financial Information Privacy Act through the legislature.

In California, business practices that could not win the interest of real consumers in the marketplace have become the law of the entire state.

Thus, business practices that could not win the interest of real consumers in the marketplace have become the law of the entire state. The California consumers who object to information sharing may have increased privacy thanks to the California law, but their numbers and the strength of their interest appears small, based on what we know from eLoan.com's anemic results.

The Regulatory Experience

More evidence about the strength of consumer interest in privacy through regulation emerges from experience at the federal level with the federal Gramm-Leach-Bliley Act (GLBA). The GLBA requires financial services companies to give consumers notice and the right to opt out of third-party information sharing. By July 1, 2001, tens of thousands of financial institutions had mailed approximately one billion notices to consumers. Along with the droves of notices came waves of press stories and agitation from anti-commerce consumer groups urging consumers to exercise their opt-out rights.

Though firm statistics are hard to come by, the uniform view is that less than 5% of consumers took advantage of the opportunity to protect their privacy from third-party information-sharing by financial services providers. The other 95% of consumers will pay extra for financial services — for notices they do not read and corporate practices they do not use — because of the GLBA regulations. And the costs of notice and opt-out procedures will recur indefinitely, compounding the harm to consumers.

Under Gramm-Leach-Bliley, less than 5% of consumers took advantage of the opportunity to protect their privacy from third-party information-sharing by financial services providers.

A wide range of factors may explain the response rates under the GLBA. One of the most likely is that consumers who trust financial institutions with their money also trust those institutions to handle information about them responsibly. Without knowing about each protection explicitly, consumers may recognize: that established companies value their reputation and brand, so will avoid harm or annoyance to customers; that companies are bound by explicit and implicit promises to protect sensitive data; that these companies bind vendors and third parties to such protections; that all legally harmful uses of information are against the law; and so on.

It is important to keep in mind that the GLBA dealt with third-party information sharing, not affiliate sharing. Third-party sharing is probably a greater focus of privacy concern than affiliate sharing, which is the subject of so much attention in the current proposals.

Given the opportunity in GLBA, the vast majority of consumers did not act to prevent sharing of information with companies and entities outside the corporate family they patronized. Preventing information sharing within corporate families is probably an even lower concern.

Apologists for the GLBA, and advocates of "notice" as a substantial privacy aid, often complain that the GLBA notices were needlessly arcane or that they were written in legalese to obscure consumers' rights. It may be true that the notices were a difficult read, but the complaint rings especially hollow now that a comparable program exists. This program has tapped into a genuine consumer interest and gotten very high response rates — *with no individualized notice at all*.

Advocates often complain that the GLBA notices were written in legalese to obscure consumers' rights. The complaint rings especially hollow now that Do-Not-Call listing has tapped into a genuine consumer interest and gotten very high response rates — *with no individualized notice at all*.

Since June of this year, the Federal Trade Commission has been compiling a list of telephone numbers whose owners do not want to be called by telemarketers. Under an FTC regulation, telemarketers must compare phone numbers on their lists to the Do-Not-Call list and leave numbers on the FTC list alone. In just a few months, the list has grown to over 50 million numbers, something like half of the telephone lines in the United States. This illustrates what happens when a genuine consumer interest is involved — response rates 10 times greater than the GLBA's third-party sharing regulation.

The Do-Not-Call list still involves substantial costs — to non-users who must pay taxes to support it for others, to users of the list who give up privacy by placing their names in a government-controlled database, to telemarketing firms and their employees, to companies that sell products via telemarketing and their employees, and to consumers who will not learn of offers they may want. The Do-Not-Call list is not preferable to the market solutions that came to the problem of unwanted telemarketing too late. But it does illustrate what happens when a consumer desire is addressed.

Recent experience with federal regulation illustrates the stark difference between what happens when a consumer interest is accurately discovered and when it is not. The GLBA's regulation of third-party sharing missed the mark. Advocates of affiliate-sharing regulation should apply the clear lessons of this experience.

Lessons from GLBA and Do-Not-Call

Differences and similarities between the GLBA and the Do-Not-Call list reveal some valuable lessons and suggest the results that can be expected from affiliate-sharing regulation.

Focus on Wrongs, Not "Rights"

The Do-Not-Call list was aimed at a misuse of information, the annoyance and irritation of unwanted phone calls. Affiliate-sharing regulation, on the other hand, is aimed at prophylactic control of information and obscure new "rights" that may or may not benefit consumers in ways that matter to them.

FTC Chairman Tim Muris summarized his successful focus on harms, rather than "rights," in an August, 2003 speech to The Progress & Freedom Foundation's Aspen Summit: "Focusing on the harms that occur when information is misused or inaccurate, rather than on notice and choice about whether the information can be collected or used at all, is a more workable approach. Concentrating on harm reflects what troubles consumers the most, while not unduly restricting the free flow of information that benefits our economy. It also imposes costs on harmful practices and the companies who use them, rather than raising the expenses of everyone engaged in commerce."[13] Do-Not-Call listing has succeeded with consumers, while affiliate-sharing regulation probably will not.

Consumers Choose Publicity as Often as Privacy

A second difference between Do-Not-Call listing and the GLBA regulation is the consequences of each for privacy. The GLBA probably marginally improved the privacy of some consumers who are highly sensitive about commercial information practices. It did not inspire consumer action. Do-Not-Call listing, although it has been touted as "privacy" protection, marginally decreases privacy,[14] and it has been enormously popular.

Shortly after the federal Do-Not-Call list went into effect, an enterprising newspaper reporter queried the database to learn that some direct marketing industry executives' numbers are on the list.[15] This cleverly exposed hypocrisy and, at the same time, made clear that placing a number on a Do-Not-Call list is actually a limited-purpose *public declaration* that the persons at a certain number wish not to receive marketing calls. People whose numbers are on the list are also subject to the risk that the government will put the list to new uses or make additional disclosures of it without

---

[13] *The Federal Trade Commission and the Future Development of U.S. Consumer Protection Policy*, Remarks by Timothy J. Muris, Chairman, Federal Trade Commission, Aspen Summit: *Cyberspace and the American Dream*, The Progress & Freedom Foundation (August 19, 2003) <http://www.ftc.gov/speeches/muris/030819aspen.htm>.

[14] *See The Price of Peace: It's Privacy*, by Jim Harper, National Review Online <http://www.nationalreview.com/comment/comment-harper052902.asp>.

[15] *Telemarketing Bosses on Do Not Call List*, Washington Times (UPI) (Oct. 1, 2003) <http://washingtontimes.com/upi-breaking/20031001-083229-3936r.htm>.

giving them choice or recourse. Consumers' privacy is slightly worse off when they add themselves to the list, but they choose Do-Not-Call all the same.

Consumers Dislike Intrusion, Less So Marketing

One similarity between Do-Not-Call listing and many of the current proposals to regulate affiliate-sharing is that they are both focused on marketing. Proponents of affiliate-sharing regulation may believe that the anti-marketing element of their proposals will make them popular, but this is not a lesson of experience. The GLBA was phrased as a general limitation on third-party sharing, but a variety of exceptions meant that, as a functional matter, it gave consumers only the power to prevent sharing for third-party marketing. Consumers were not motivated by the opportunity to reject marketing that they were offered in GLBA. They were motivated by the opportunity to avoid intrusion that they got with Do-Not-Call.

On balance, affiliate-sharing regulation appears unlikely to tap into real consumer desire. Advocates and politicians who claim to be protecting consumers with affiliate-sharing regulation certainly have a wealth of conventional wisdom to support them. But the best evidence available about what motivates consumers does not support the notion that affiliate-sharing regulation will benefit the majority. Instead, affiliate-sharing regulation appears likely to impose costs on all consumers in order to serve the preferences of a narrow group of privacy outliers.

Conclusion

In the name of privacy, a spate of regulations has been aimed at commercial information practices. It is important to examine whether they actually promote privacy, and how well.

Privacy is the condition people enjoy when they have power to control information about themselves and when they do so consistent with their interests and values. Affiliate- and third-party sharing regulations may advance the privacy of some consumers, but the number of consumers who would benefit is debatable.

The evidence that is available from both marketplace experience and prior regulation shows that affiliate-sharing is probably not a great interest or motivator of most consumers. By comparing experience under the Gramm-Leach-Bliley Act with the federal Do-Not-Call list, several lessons emerge.

First, abstract "privacy rights" do not appeal to consumers the way protection from real harms does. Real consumer advocacy should focus on what real consumers really want. Second, consumers sometimes give up privacy and choose publicity to get the things they want. There is nothing inherently wrong with this choice; it is one for consumers to make. Third, consumers have a strong dislike for intrusive marketing that may not extend to marketing as a whole. Thoughtful people will not take the success of Do-Not-Call listing as a signal that consumers reject all marketing.

Increasingly, of late, the privacy debate has devolved into a debate about marketing. Some pro-regulation privacy activists have used the word "privacy" as a cover for anti-commercial and anti-marketing public policies. Marketing should be the subject of debate and discussion, but directly on its own terms — not under the cover of the word "privacy."

Too many genuine privacy issues remain to let an anti-marketing agenda dominate our national discussion about privacy. The tax code and our nation's entitlement programs still require reams and reams of personal information to be taken from our control. The federal government continues to advance programs like the Financial Crimes Enforcement Network, CAPPS II, and Total Information Awareness. Daily *Federal Register* notices announce new uses of personal information by federal agencies. And information-transfer from the private sector to the public sector continues to threaten privacy and civil liberties. These areas, where consumers and citizens lack power and choice, should be the focus of continued and renewed privacy efforts.

In the meantime, politicians who seek to regulation corporate information practices are merely diverting attention from the more serious privacy threats from government — threats that they are responsible for creating and maintaining.