

Senate Commerce Committee
Hearing on
INTERNET PRIVACY
July 11, 2001

Prepared Statement of Professor Fred H. Cate

Mr. Chairman:

My name is Fred Cate, and I am a professor of law and director of the Information Law and Commerce Institute at the Indiana University School of Law in Bloomington, and Global Information Policy Advisor to the law firm of Hunton & Williams. For the past 12 years, I have researched, written, and taught about information laws issues generally, and privacy law issues specifically. I directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, served as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and currently am a visiting fellow, addressing privacy issues, at the American Enterprise Institute.

I appreciate the opportunity to testify today. I would like to take advantage of the presence of my distinguished colleagues on this panel and limit my testimony to two points: the ways in which requiring consumer "consent" for information collection and use burdens consumers and creates costs, and the extent to which requiring opt-in exacerbates, rather than ameliorates, the harmful impact of many privacy laws.

The Transformation of Privacy Law

Historically, U.S. privacy law focused on two broad themes. The first and most visible was preventing intrusion by the *government*. This is the context of virtually all constitutional privacy rights, and it reflects the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance, and only the government collects and uses information free from market competition and consumer preferences.

The second theme reflected in U.S. privacy law throughout the last century was preventing uses of information that *harm* consumers. When privacy laws did address private-sector behavior, they were designed to prevent specific, identified harms. So, for example, the common law privacy torts of intrusion, public disclosure, and false light privacy all require that the conduct complained of be "highly offensive to a reasonable person,"¹ and the information disclosed must either be false² or "unreasonably place[] the other in a false light before the public."³ Similarly, the Fair Credit Reporting Act, one of earliest privacy laws applicable to the private-sector, focuses primarily on correcting inaccuracies and assuring that credit information is not used in ways likely to harm consumers.⁴

Increasingly, however, the dominant trend in recent and pending privacy legislation is to invest consumers with near absolute *control over information* in the marketplace—irrespective of

whether the information is, or could be, used to cause harm. Public officials and privacy advocates argue that “we must assure consumers that they have full *control* over their personal information”⁵ and that privacy is “an issue that will not go away until every single American has the right to *control* how their personal information is or isn’t used.”⁶ The National Association of Attorneys General’s December 2000 draft statement on Privacy Principles and Background sets forth as its core principle: “Put simply, consumers should have the right to know and *control* what data is being collected about them and how it is being used, whether it is offline or online.”⁷ And virtually all of the privacy bills pending before Congress reflect this goal: “To strengthen *control* by consumers” and “to provide greater individual *control*.”⁸

This dramatic expansion from focusing on information privacy only in the contexts of *government* collection and *harmful* use, to regulating *all* personal information in the marketplace, poses many issues. Two of the most important involve the capacity and desire of most individuals to exercise control over information about them, and the impact of the legal means by which they seek to do so.

The Limits of Control

The problem is that most consumers, in practice, don’t want to exercise that control over the information we disclose and generate. We don’t want to take the time to make those decisions, we often lack the knowledge or experience to understand the decisions we are being asked to make, we rarely want to be held responsible for the consequences of our decisions (especially since we seldom understand them), and, most significantly, we consider the interruption of being asked a nuisance and, as a result, we resent it. This is especially true on the Internet, where speed and convenience are most highly valued.

In practice, consumers ignore virtually all privacy notices and authorizations. The U.S. Post Office reports that 52% of unsolicited mail in this country is discarded without ever being read.⁹ This is especially true online. Unsolicited e-mail, even when sent by a company with which the recipient has a relationship, is *not* opened at about the same rate, privacy policies are widely ignored, and pop-up screens with terms and conditions are simply clicked through without ever being read. The chief privacy officer of Excite@Home told a Federal Trade Commission workshop on profiling that the day after *60 Minutes* featured his company in a segment on Internet privacy, only *100* out of *20 million* unique visitors accessed that company’s privacy pages.¹⁰

All of the available data on consumers opting out or opting in reflects this. Extensive experience with company-specific and industry-wide opt-out lists, and the recent experience of financial services companies providing opt-out opportunities in compliance with the privacy provisions of the 1999 Gramm-Leach-Bliley Financial Services Modernization Act, demonstrate that less than 10% of the U.S. population ever opts out of a mailing list—often the figure is less than 3%.¹¹ Privacy advocates often point to these figures as evidence that opt-out doesn’t work. However, opt-in rates are virtually identical if not lower. In fact, two major U.S. companies

recently tested the response rates to opt-in and opt-out, by sending e-mail messages describing the same use of personal information to statistically similar subsets of their respective customer bases. One e-mail said that the information would be used unless the customer opted out. The other said the information would not be used unless the customer opted in. *In both tests, the response rates were the same for both sets of messages: customers did not respond to either.*

The Opt-Out–Opt-In Comparison

The question then for Congress, as you consider the need for any new online privacy legislation and the relative merits of opt-in and opt-out, is what is the impact of any new law on consumers, *especially in light of consumers' tendency to fail to respond to privacy notices of any form.* Both opt-in and opt-out give consumers the same legal control about how their information is used; under either system, it is the customer alone who makes the final and binding determination about data use. Therefore, the real focus of your inquiry must be on the burdens and costs imposed by each system.

While I and others have written and length about these issues in broad terms, I thought it would be most useful today to try to address these questions in the most specific manner possible.

Let's assume that Congress passes a law requiring that Web site operators provide a privacy notice and obtain some form of consent before collecting, using, or disclosing personal information. What would this mean in practice?

- Opt-out

If *opt-out*, then the notice would be provided—much like 88% of commercial Web sites (100% of the busiest commercial Web sites) already do voluntarily and have done for more than a year¹²—in whatever form and including whatever terms Congress or federal regulators required. The notice would include information about opt-out opportunities. That small percentage of the public who is acutely privately sensitive and today exercises opt-out opportunities whenever presented, would continue to do so and, importantly, would for the first time have the legal right to do so.

Most consumers, however, would continue to ignore both the notices and the opt-out opportunities, precisely as they do today. And, as a result of consumers not opting out, Web sites would be free to use information for any purpose that was within the scope of the privacy notice and that was not specifically prohibited by other laws. Consumers would get the same service, benefits, opportunities, and offers that depend on that information. *This is presumably what those consumers want, because if they did not, and if they felt sufficiently strongly about it, they could exercise their opt-out right at any time.*

Given the fast-changing nature of Internet services and technologies, it is unlikely that any privacy notice would cover all future uses of information. As new uses were developed, the Web

site would be required to provide some form of prominent notice on the Web site or via e-mail (the precise details of how the notice must be provided would likely be set by federal regulators). That notice would specify both a meaningful opportunity for consumers to opt out and a sufficient amount of time for consumers to exercise their opt-out rights, before engaging in the new use. Again, it is reasonable to assume that most consumers would ignore the notice and the opt-out, but they would nevertheless receive whatever benefits or opportunities resulted from the use of their information. That is how online opt-out would work.

- Opt-in

If Congress' new law required *opt-in* consent for data collection, use, or transfer, the result would be quite different. Under opt-in, Web sites could no longer provide their privacy notices as they currently do or as they would under mandated opt-out, but instead would have to force every consumer to see the notice in an effort to obtain his or her consent to collect and use personal information. Presumably, the same small percentage of consumers who already read notices and worry about their privacy would continue to read privacy notices, but now they would have to do nothing to block use of their information. The substantial majority of other consumers who ignore privacy policies would also likely continue to do so.

Assuming the information was necessary to provide the service (for example, an address necessary to mail a book or airline ticket) or that the Web site chose to condition service on the consumer opting in, then the failure to opt in would mean no service. Both the minority of consumers who act on privacy policies, and the majority of the rest of us who simply ignore them, would be denied service. *Our privacy would be protected to be sure, but at the price of our not using the Internet.* Consumers can obtain this type of privacy protection today—just by walking away from businesses whose privacy policies we disagree with—without the intervention of Congress.

For a sense for what this would be like in practice, set your browser to ask before accepting cookies. After you have been interrupted 10 or 12 times asking for consent to record information that is *necessary* to access the requested site, you will have a good feeling for what opt-in is like. If you click “No,” you will be blocked from the Web page, so while you may have the satisfaction of being asked—again and again—you have no choice but to consent, unless you want to seek service elsewhere. *After having our Internet browsing repeatedly interrupted by opt-in requests to which we must accede to proceed, most Americans will be asking how to opt out of opt-in.*

As new uses for the information were developed, the operator would have to contact every consumer individually to ask him or her to opt in to the proposed use of the information. When most consumers failed to respond, presumably the Web site operator would try again and again to gain consent, thus increasingly burdening the consumer with more unsolicited e-mail, telephone calls, and/or mail, and increasing the cost of providing the new service or product for which consent was being sought.

We have some sense of what that cost and burden might amount to. U.S. West, one of the few U.S. companies to test an opt-in system, found that to obtain permission to use information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.) to market services to them required an average of 4.8 calls to each customer household before the company reached an adult who even could grant consent, and cost almost \$30 per customer contacted.¹³ Some of those calls went unanswered, but others reached answering machines, children, and other household members and visitors who were ineligible to consent. Those individuals bore the burden resulting from the practical fact that it is much harder for businesses to contact consumers than for consumers to contact businesses—but this is precisely what opt-in requires.

A 2000 Ernst & Young study of financial institutions representing 30% of financial services industry revenues, found that financial services companies would send out *three to six times* more direct marketing material if they could not use shared personal information to target their mailings, at an additional cost of about \$1 billion per year.¹⁴ The study concluded that the total annual cost to consumers of opt-in's restriction on existing information flows—precisely because of the difficulty of reaching customers—was \$17 billion for the companies studied, or \$56 billion if extrapolated to include the customers of all financial institutions. And those figures do not include the costs resulting from restricting information-flows to reduce fraud, increase the availability and lower the cost of credit, provide co-branded credit cards and nationwide automated teller machine networks, develop future innovative services and products.¹⁵

The reason for this greater cost is easy to see. Under opt-out, a business wishing to use information about consumers can inform all potential consumers at once—through policies posted on Web sites, disclosures mailed to customer addresses, and other efficient, cost-effective forms of communications. The business doesn't even have to know specifically with whom it is attempting to communicate.

Consumers who object to a proposed use of personal information can prevent it by contacting the business via a toll-free telephone number, Web site, or pre-addressed response card. The communication can take place at virtually anytime—and therefore at the consumer's convenience—and the response mechanism can serve other business purposes. For example, the 800-number can reach a customer service center that is staffed to answer a variety of customer questions and provide access to customer account information. The Web site can provide a wide range of information and services, in addition to the opportunity to opt-out.

The comparative ease of communicating the privacy notice to the consumer, the flexibility of the customer being able to opt-out at his or her convenience, and the ability to spread the cost of handling "opt-outs" using systems that serve other functions does not mean that opt-out is without cost, but it does help to reduce those costs—both to consumers and businesses—significantly.

Moreover, the burden on consumers is multiplied by the fact that all of these contacts are just to obtain permission to examine data about customers to determine their eligibility for a product or service offering. For those individuals who are eligible, a *second* round of contacts is necessary to

actually make them to offer. It is difficult to imagine that this opt-in system will be perceived by consumers as anything more than an annoyance. U.S. West's customers displayed their annoyance at the intrusiveness required by opt-in. Only 28% opted-in when they were interrupted with a call seeking consent, but 72% opted-in when the opportunity to consent was presented to the customer at the conclusion of a call that the *customer* initiated.¹⁶

Of course, this annoyance will be even greater for those people who do *not* qualify for the offer. For example, in the case of U.S. West, the telephone company was asking existing customers for permission to examine information about their calling patterns to determine their eligibility for new service plans and discounts. However, not all customers who consented actually qualified for the new service or discount. The burden and cost of contacting those customers who did *not* qualify were wholly wasted.

Under opt-in, the Web site operator has to contact all customers seeking their individual consent to examine data about them, even though many or most may not qualify for the offer. Because opt-in prevents businesses from using personal information to target their consent requests, it not only results in extra contacts with the consumers, but also exacerbates the burden of those contacts because they cannot be tailored to reflect consumer interests.

These same issues are presented by efforts to attract *new* customers by using personal information (such as their e-mail address) to contact them. Today, if a company wishes to expand into a new geographic area or product line, it may seek a list of potential customers from a third party. Under *opt-out*, a third party is free to provide the company with such a list, provided that it excludes consumers who have already opted-out of receiving such communications. The company can then use the list to contact people with a special offer or introductory discount. After receiving the offer, consumers are free to opt-out of receiving future offers from that company. The only "harm" suffered by the individual is receiving an offer in which he or she ultimately was not interested.

Under *opt-in*, every person on that list will need to be contacted for consent. The company *cannot* contact them, because it does not have explicit consent to make such a use of their names or addresses. The third party supplying the list is unlikely to bear the expense and inconvenience of contacting every person on the list. The promise of explicit consent in the opt-in requirement has resulted in nothing to consent to at all.

Alternatively, depending upon the specific requirements of the opt-in law, the new service provider may be allowed to contact potential customers, but it will have to do so twice: once to gain consent to make the second contact conveying the offer. Moreover, since most requests for consent are ignored, the most likely effect on an opt-in law is to prevent contacting potential customers entirely. This is why Robert E. Litan, Director of the Economic Studies Program and Vice President of The Brookings Institution, 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."¹⁷

Opt-In and the Illusion of Consent

Because of the inherent difficulty of businesses contacting consumers individually, many consumers may miss out on opportunities that they would value, not because they chose not to receive them, but because they *never had the opportunity to choose*. In one-third of households called by U.S. West, for example, the company *never reached the customer*, despite repeated attempts. Consequently, those customers were denied the opportunity to receive information about new products and services.¹⁸ This is a very practical example of the way in which an opt-in system may only create the *illusion* of consent.

We have already seen the extent to which consumers ignore requests for consent. Moreover, even when mail is actually read and the offer appeals to the consumer, lethargy and the competing demands of busy lives often conspire to ensure that no action is taken. Only 6-11% of customers in the U.S. West opt-in test responded to written opt-in requests, even though more than four times that number—28%—indicated that they desired the service when called about it, and, as noted, 72% ordered the service when asked during a phone call that the customer initiated.¹⁹ This suggests that the issue isn't privacy or the attractiveness of the request, but rather the annoyance to consumers of being interrupted with requests for consent—precisely what an opt-in law contemplates.

The opportunity to consent may also be illusory because the business wishing to use the information has no affordable way of reaching consumers individually. If the cost of obtaining consent is too great to make the proposed use of information economically feasible, then there will be nothing to which the consumer can consent.

If opt-in means that lists of potential customers are no longer available from third parties, then, as we have seen, the promise of explicit consent in the opt-in requirement will likely result in nothing to consent to at all. Consider the example of AOL Time Warner. As a start-up company, AOL mailed free copies of its software to people likely to be interested in Internet access. Prohibiting the fledgling AOL access to information about consumer addresses and computer ownership would have denied consumers information about an opportunity that many of them obviously value, increased the volume of marketing material that AOL would have been required to distribute, and threatened the financial viability of a valuable, innovative service.

The opportunity for consent under an opt-in system may also be illusory because of the difficulty of building new data systems, and implementing new uses of data, one customer at a time. For example, highly valued services, such as consolidated statements and customer service, could not exist if consumers were given the choice about the sharing of information about their accounts, because few businesses could realistically provide both consolidated and nonconsolidated services. To do so would require one customer service center manned by one set of representatives using one information system for customers who consented to information-sharing, and a panoply of other customer service centers manned by teams of other representatives using a variety of other information systems each covering only a single aspect of a customer's account for those customers who did not consent. This is an area where there is *no* room for consumer choice—opt-in or opt-out: Service must either be

provided on a consolidated basis for all (which is the choice of most consumers) or for none (in which cases all customers must endure the added cost and inconvenience of separate statements and service centers).

Finally, as noted, the opportunity for consent is always illusory if the service or product *cannot* or *will not* be provided without personal information. I experienced a very practical example of this just this past weekend. When downloading software, I was presented with a pop-up privacy policy. I could not continue installing the software I wanted without providing the information requested—the site needed to know certain information about my system to know which software to send and how to configure it— and without clicking on the “I accept” button. The presence of that policy was a small burden and annoyance, but yielded no benefit. *The opportunity to opt in meant nothing—was wholly illusory— because consent was a condition of service.* A law requiring opt-in consent in that situation would have merely increased the cost and burden of formally verifying and recording the consent that I had already manifest by my behavior, to use information without which the requested service could not have been provided.

The Lesson From Europe

A number of legislators and privacy advocates have argued that since the use of personal information in Europe is conditioned on opt-in consent, the burdens and costs of opt-in must not be as great as research and experience have suggested. This argument is fundamentally flawed, as we are learning.

While it is true that European nations are required under the European Union data protection directive, which took effect in 1998, to condition the collection, use, or transfer of personal information on explicit opt-in consent,²⁰ there is little evidence that any have, in fact, done so. European data protection officials have repeatedly pointed out the impossibility of doing so. Instead, Europe has used a concept of “implied explicit consent”—if individuals are told of the intended data collection or use and do not object, then surely, European data protection officials argue, they must have opted-in. There is nothing to distinguish this from opt-out. Privacy scholar Amitai Etzioni has noted that European citizens rarely, if ever, are asked for explicit permission to use personal information about them. In fact, he tells of regularly asking his European audiences if anyone has ever been asked to opt-in. To date, Etzioni reports only one positive response—from a man who was asked for opt-in consent by Amazon.com, a U.S. company.²¹ “It seems that this EU directive is one of those laws that is enacted to keep one group—privacy advocates and their followers—happy and, as a rule, is not enforced so that commerce and life can continue.”²²

A January 2001 study by Consumers International bears out Etzioni’s conclusion. Consumers International examined the use and protection of personal information on 751 retail, financial, health, and other popular Web sites in the United States and Europe. The study found that while U.S. and European Web sites collect personal information at nearly comparable rates (66% in the United States; 63% in Europe), U.S. sites provide better privacy protection, despite having no specific legal obligation to do so, than European sites, which are subject to comprehensive legal requirements:

Despite tight EU legislation in this area, researchers did not find that sites based in the EU gave better information or a higher degree of choice to their users than sites based in the US. *Indeed, US-based sites tended to set the standard for decent privacy policies.*²³

Ironically, not only have more restrictive laws failed to provide a higher standard of privacy protection, they have also failed to quell consumer fears. Polls on consumer privacy concerns show nearly identical results in the United States and Europe, despite wide differences between laws. For example, Lou Harris & Associates found in 1999 that 80% of U.S. consumers and 79% of German consumers surveyed agreed with the statement “consumers have lost all control over how personal information is collected and used by companies.”²⁴ Similarly, 71% of the U.S. sample and 70% of the German sample agreed that “it is impossible to protect consumer privacy in the computer age.”²⁵ In fact, despite the far greater legal protections for privacy available in Europe, Americans (64%) were *more* likely than Germans (55%) or British (58%) respondents to believe that businesses will handle personal information in a “proper and confidential way.”²⁶ However, Americans (29%) proved no more likely than Germans (28%) and only slightly more likely than the British (23%) to say they personally have been a victim of what they felt was an improper invasion of privacy by a business.²⁷

Opt-In and the First Amendment

Opt-in also poses significant constitutional issues under the First Amendment. The Supreme Court has struck down many ordinances that would require affirmative consent before receiving door-to-door solicitations,²⁸ before receiving Communist literature,²⁹ even before receiving “patently offensive” cable programming.³⁰ The Court’s opinion in the 1943 case of *Martin v. Struthers*—involving a local ordinance that banned door-to-door solicitations without explicit (opt-in) householder consent—is particularly apt:

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.³¹

The only federal court to review a modern opt-in requirement concluded that it violated the First Amendment. In 1999, the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc. v. Federal Communications Commission*, struck down the Commission’s rules requiring that telephone companies obtain explicit consent from their customers before using data about those customers’ calling patterns to market products or services to them.³² The court found that the FCC’s rules, by limiting the use of personal information when communicating with customers, restricted U.S. West’s speech and therefore were subject to First Amendment review. The court determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a “*specific and significant harm*” on

individuals, and that the rules were “no more extensive than necessary to serve [the stated] interests.”³³

Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* [the test applicable to commercial speech] for it is not based on an identified harm.³⁴

The court found that for the Commission to demonstrate that the opt-in rules were sufficiently narrowly tailored, it must prove that less restrictive opt-out rules would not offer sufficient privacy protection:

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.*³⁵

The court found that the FCC had failed to show why more burdensome opt-in rules were necessary, and therefore struck down the rules as unconstitutional. The Supreme Court declined to review the case.³⁶

The Tenth Circuit’s opinion in *U.S. West* is particularly applicable to the current debate over opt-out and opt-in because it reaffirms what the Supreme Court had previously indicated: that opt-in is more burdensome than opt-out, and that, as a result, for the government to adopt opt-in rules, it must first demonstrate that opt-out is not adequate.

Conclusion

- The Role of Opt-In

Opt-in has its place. For example, Congress wisely required the explicit consent of parents before Web sites collected information from very young children.³⁷ Information that is particularly sensitive or particularly likely to be misused to harm the individual might also be subjected to opt-in consent. And some companies online today voluntarily use opt-in in settings where it is most easily managed (such as online service providers, which by definition have contact with their customers every time they log on) or where it is necessary to ensure consumer confidence given the sensitivity of the relationship and information (such as certain financial and health sites). But in other settings, the higher costs imposed by a legally mandated opt-in system are unwarranted.

This is especially true on the Internet where much of the information disclosed is not sensitive or likely to be used to harm the individual, but rather is a substitute for the very address information browsing and buying habits that store clerks and merchants have been noting for years. Moreover, because the use of information is so central to customer service and convenience online, and the very attraction of the Internet is its speed and ease-of-use, opt-in as a legal requirement seems peculiarly inappropriate in the context of the Internet.

Opt-in is unlikely to enhance privacy protection, because consumers asked to opt in prior to receiving service are likely to do so to receive service and to avoid the annoyance of being asked again. (That is why millions of us click “I accept” boxes without ever reading the terms to which we are agreeing.) Consumers asked to opt in later to new uses of information are in most settings unlikely to ever be aware of the request. This suggests that simply conditioning the use of personal information on specific consent is tantamount to either creating a hoop that Web users *must* jump through to obtain access to the information and services they desire, or, alternatively, to effectively *prohibiting outright* many beneficial uses of information. In either case, opt-in acts like a *tax* on online commerce, compelling all consumers to pay for the heightened privacy concerns of a few, yet providing enhanced privacy to no one.

- The Role of the Government

The fact that opt-in laws do not appear generally appropriate or necessary for protecting privacy on the Internet, does not mean that there is no role for the government or for law in protecting privacy online. Far from it.

Regulators and law enforcement officials should enforce existing privacy laws vigorously, and legislators should ensure that they have the resources to do so. This is especially important in the context of the Internet, where disparate jurisdictions and laws can make enforcing existing laws difficult for most consumers. I think it is especially important for the government to help ensure that Web sites adhere to the commitments that they make in their privacy policies—whether those policies are voluntary or required by law—so that individuals who do read those policies can rely on them with confidence.

The government should also help educate the public about privacy and the tools available to every citizen to protect our own privacy. Many privacy protections can only be used by individuals—no one else can protect their privacy for them. This is especially true on Web sites, a majority of which originate in countries outside of the United States. The common sense steps and practical technologies that individuals can employ to protect themselves offer better, more effective protection than any law. Yet few individuals will recognize the importance of their responsibility or have the knowledge to fulfill it without education.

Finally, should Congress conclude that some form of new mandated consent requirement is necessary, *opt-out* is the less burdensome alternative and the one more likely to be effective. It allows people who are most concerned about their privacy to act to protect it—using the same legal right that

they have with opt-in—without unduly burdening the great majority of us who are unlikely to read or act on privacy notices. You may wish to take steps to make privacy notices more complete and clear, and opt-out more effective. I advise caution, however, before substituting Congress' judgment for that of the market. Remember, the Gramm-Leach-Bliley privacy notices that the press and state legislatures are so busy criticizing, were largely written by federal regulators. Their complexity is precisely what we should expect if we require those notices to comply with federal regulations and regard them as creating binding contracts. Before mandating such notices online, I urge you to think carefully about whether there is any certain way to do better, and whether the cost of doing so is justified in light of the few consumers who will ever read them.

Thank you again for the opportunity to testify.

Biographical Statement

Fred H. Cate is a professor of law, Ira C. Batman Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington. He is also Global Information Policy Advisor to the law firm of Hunton & Williams and a visiting scholar at the American Enterprise Institute.

Professor Cate is a recognized authority on privacy and other information law issues. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution; chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities; served as vice chair of the American Bar Association Section on Health Law's Electronic Communications and Privacy Interest Group; and was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. During the 2000 presidential race he advised the George W. Bush campaign on privacy matters.

Professor Cate is the author of many articles and books concerning privacy and information law, including *Privacy in Perspective* (AEI Press), *Privacy in the Information Age* (Brookings Institution Press), and *The Internet and the First Amendment* (Phi Delta Kappa). He is the co-author of the sixth edition of the best-selling *Mass Media Law* (Foundation Press) (with Marc Franklin and David Anderson).

A graduate of Stanford University and Stanford Law School, Professor Cate is a member of the Phi Beta Kappa Senate and of the board of directors of the Phi Beta Kappa Fellows, and is listed in *Who's Who in American Law*.

He may be contacted at the Indiana University School of Law—Bloomington, 211 South Indiana Avenue, Bloomington, IN 47405-7001, telephone (812) 855-1161, facsimile (812) 855-0555, fcate@indiana.edu.

Notes

1. Restatement (Second) of Torts §§ 652B, D-E (1976).
2. Philadelphia Newspaper, Inc. v. Hepps, 475 U.S. 767, 777 (1986).
3. Restatement, supra, § 652E.
4. 15 U.S.C. § 1681b(a) (1999).
5. Enactment of the Children's Online Privacy Protection Act, 106th Congress, 2d Session, 146 Cong. Rec. E616, May 2, 2000, statement of Jay Inslee (D-Wash.) (emphasis added).
6. Democrats Hold News Conference on Financial Privacy, May 4, 2000 (statement of John LaFalce (D-N.Y.)) (emphasis added).
7. National Association of Attorneys General, supra at 7 (emphasis added).
8. S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong. § 2(b)(1) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001) (emphasis added)
9. "Briefs," Circulation Management, May 1999 (referring to the U.S. Postal Service's Household Diary Study (1997)).
10. Federal Trade Commission, Workshop on The Information Marketplace: Merging and Exchanging Consumer Data, Mar. 31, 2001 (comments of Ted Wham).
11. Less than 3% of the U.S. population takes advantage of the Direct Marketing Association's Mail and Telephone Preference Services. Financial 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 20, 1999) (statement of Richard A. Barton) (available at <http://www.house.gov/banking/72099rba.htm>). Financial institutions, retailers, and other businesses report similar or lower figures for their opt-out programs.
12. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* at 11 (2000).
13. Brief for Petitioner and Interveners at 15-16, U.S. West, Inc. v. Federal Communications Commission, 182 F.3d 1224, 1239 (10th Cir. 1999) (No. 98-9518), cert. denied 528 U.S. 1188 (2000).
14. Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies* 16 (Dec. 2000).
15. Id.
16. U.S. West, Inc. v. Federal Communications Commission, 182 F.3d 1224, 1239 (10th Cir. 1999), cert. denied 528 U.S. 1188 (2000).

17. Robert E. Litan, Balancing Costs and Benefits of New Privacy Mandates, in Lucien Rapp & Fred H. Cate, *European and U.S. Perspectives on Information Privacy* (forthcoming).
18. Brief for Petitioner and Interveners at 15-16, U.S. West, *supra*.
19. *U.S. West*, 182 F.3d at 1239.
20. Directive 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. 7 (Eur. O.J. 95/L281).
21. Personal communication from Amitai Etzioni to the author (Feb. 21, 2001).
22. Amitai Etzioni, "Protecting Privacy," *Financial Times*, April 9, 1999, at 18.
23. Consumers International, *Privacy@net: An International Comparative Study of Consumer Privacy on the Internet* at 6 (2001) (emphasis added).
24. *IBM Multi-National Consumer Privacy Survey* at 22 (1999).
25. *Id.*
26. *Id.*
27. *Id.* at 14.
28. *Martin v. Struthers*, 319 U.S. 141 (1943).
29. *Lamont v. Postmaster General*, 381 U.S. 301 (1965).
30. *Denver Area Educational Telecommunications Consortium, Inc. v. Federal Communications Commission*, 518 U.S. 727 (1996).
31. *Martin*, 319 U.S. at 141.
32. *U.S. West*, 182 F.3d at 1235.
33. *Id.* at 1235 (quoting *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 486 (1995)).
34. *U.S. West*, 182 F.3d at 1235 (emphasis added).
35. *Id.* (emphasis added).
36. *U.S. West Communications, Inc. v. Federal Communications Commission*, 528 U.S. 1188 (2000).
37. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (codified as amended at 15 U.S.C. §§ 6501-06 (1999)).