

Senate Commerce Committee Hearing on
THE ONLINE PERSONAL PRIVACY ACT
April 25, 2002

Written Testimony of Professor Fred H. Cate¹

Introduction and Summary

The Online Personal Privacy Act (the “Act”) pending before the Commerce Committee (the “Committee”) seeks to protect the privacy of information about individuals collected online. The Act is unlikely to achieve this important goal for six interrelated reasons:

1. The Act lumps together all forms of information collection and use online without regard for whether the information was provided or observed, whether the individual user was aware of the collection, whether there was a pre-existing relationship, the potential of the information to cause harm, or the context in which it was collected. Liability is imposed under a strict-liability regime, irrespective of intent, reasonableness, or whether a violation of the Act causes harm.
2. The Act relies on regulatory tools that have a demonstrated track-record of failing to protect privacy. Some of those tools, for example, mandatory access, may actually create new privacy risks.
3. The Act is unnecessarily complex and bureaucratic, for example, requiring three types of notice and two types of consent, and employing three different enforcement mechanisms.
4. Many of the Act’s requirements are impractical; some, such as sending notices to people for whom no contact information has been collected, are impossible. In several cases, such as implementing access and security requirements, the Act requires providers of Internet and online services and operators of commercial websites to discover solutions to problems that so far have evaded Congress and the Federal Trade Commission (“FTC” or the “Commission”).
5. Even if the Act’s provisions proved effective, they create inconsistent privacy protections that would treat information collected online differently from information collected offline, subject commercial websites to different requirements than noncommercial, and imposes conflicting requirements on entities subject to existing federal and state privacy laws.

¹Professor of law, Ira C. Batman Faculty Fellow, and director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington; senior policy advisor, Hunton & Williams Center for Information Policy Leadership; and visiting scholar, American Enterprise Institute. Professor Cate directed the Electronic Information Privacy and Commerce Study for the Brookings Institution; 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. He is the author of many articles and books concerning privacy and information law, including *Privacy in Perspective*, *Privacy in the Information Age*, *The Internet and the First Amendment*, and *Mass Media Law* (6th ed.) (with Marc Franklin and David Anderson). This written testimony is submitted on his own behalf; the views expressed herein should not be attributed to any institution with which he is affiliated.

6. Finally, many terms in the Act are vague or undefined. These drafting failures exacerbate the Act's other weaknesses, and cause the Act to reach far more broadly than might first appear.

Rather than enhance privacy protection online, the Act creates new, often incomprehensible barriers to consumer access to Internet content that are more likely to frustrate consumers, raise the cost of that access, reduce innovation in online services and products, and create unconstitutional impediments to Internet expression.

The Act

The Online Personal Privacy Act prohibits providers of Internet or online services, including commercial websites, from collecting, using, or disclosing information online unless they:

- Notice (1)—Provide “clear and conspicuous” notice (§ 102(a));
- Notice (2)—Provide “robust” notice whenever information is collected (§§ 102(c)-(d));
- Consent—Obtain “affirmative consent” if the information is “sensitive” (§ 102(b)), or provide an opportunity to “decline consent” for other information (§ 102(c));
- Exceptions—There are exceptions to these three requirements for collecting, using, or disclosing information online that is necessary:
 - to “protect the security or integrity” of the service or the “safety” of people or property (§ 104(a)(1));
 - to “conduct a transaction, deliver a product or service, or complete an arrangement for which the user provided the information” (§ 104(a)(2));
 - to provide products or services “integrally related” to such an activity (§ 104(a)(3));
 - to comply with a “request or demand” for the information from the government (§ 104(c)(1)(A)); or
 - in response to a civil court order, if specified conditions are met. (§ 104(c)(1)(B)).
- Notice (3)—Provide an unspecified level of notice upon any “material change” in privacy policy, any violation of the Act, or in the event the “security, confidentiality, or integrity” of the information is compromised (§ 103(a));
- Access and Correction—Provide access and an opportunity to “suggest a correction or deletion” of collected information (§ 105); and
- Security—Maintain “reasonable procedures” necessary to protect the “security, confidentiality, and integrity” of information (§ 106).

Any violation of the Act is subject to investigation and suit by the FTC as an “unfair or deceptive” act (§ 202(a)) (or, with regard to entities subject to their respective jurisdiction, by the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration Board, the Secretary Transportation, the

Secretary of Agriculture, or the Farm Credit Administration, as a substantive violation of their respective enabling acts (§ 202(b)); private lawsuits if the information involved is “sensitive” (§ 203); and lawsuits by state governments (§ 204).

Penalties for violation of the Act include any of the civil or criminal penalties that the FTC or other agency specified above may lawfully pursue, including fines, injunctions, and imprisonment; if the information is “sensitive” and the violation causes “actual harm,” the greater of actual monetary loss or statutory damages of \$5,000, which may be increased to \$100,000 for “repeated[] and knowing[]” violations (§ 203); and any civil penalty that a state attorney general is permitted by law to seek (§ 204).

The Act also:

- preempts any state “statute, regulation, or rule regulating Internet privacy to the extent that it relates to the collection, use, or disclosure” of information subject to the Act (§ 4);
- extends the effect of consent provided to one party to other “successor” parties, provided that the kind of information collected, the means of collection, and the “disclosure practices” of the successor are not materially different (§ 102(e));
- extends the Act to federal agencies (§ 302) and, by internal regulation, to the Senate (§ 301);
- requires the FTC to establish a procedure for distributing civil penalties to individual Internet users (§ 202(c));
- provides “whistleblower protection” for employees of providers who are fired or discriminated against because they report violations of the Act to the government (§ 205);
- directs the FTC to report on the need for, and application of, the Act, and whether such a law is necessary for information collected offline (§ 404); and
- amends the National Institute of Standards and Technology Act to require the Institute to “encourage and support” the development of technologies for protecting privacy online (§ 405).

Assessment of the Act

Scope and Vagueness

The Act is very broad, even broader than may first appear because of its reliance on vague and undefined terms. The Act applies to all “internet service providers” and “online service providers,” whether or not commercial, and to the operators of “commercial websites” (§ 101(a)), although the Act does not define any of these key terms (§ 401(8)). It also applies to anyone—without apparent limit—who “uses an internet service provider, online service provider, or commercial website operator to collect information about users of that service or website” (§ 101(b)). There is no explanation of what “uses” means in this context, but given the breadth of definition of “collect”—which includes “direct or indirect, active or passive” gathering of

information (§ 401(1)) (discussed below)—it seems likely that the Act applies to anyone who obtains information from a provider or operator.

The Act applies to “personally identifiable information” that is collected online. This term is given an expansive definition to include (a) basic information (such as name, address, and telephone number) that is routinely made available publicly (§ 401(11)(A)); (b) “any other identifier for which the Commission finds there is a substantial likelihood that the identifier would permit the physical or online contacting of a specific individual” (§ 401(11)(A)(vi)); and (c) any information that a provider collects from any source and combines with personally identifiable information collected online (§ 401(11)(A)(vii)). The absence of the word “online” in the phrase “from any source” in the third definition raises the risk that the might apply to certain offline data. In any event, the breath of the Act means that the Act will overlap, and likely conflict, with other federal and state privacy statutes and regulations, such as the Gramm-Leach-Bliley Financial Services Modernization Act and the privacy rules adopted pursuant to the Health Insurance Portability and Accountability Act, which apply both online and offline.

As noted, the term “collect” is defined to include the gathering of information “by any means, direct or indirect, active or passive” (§ 401(1)). The Act includes examples of only active information gathering, but the definition would cover, for example, any provider or operator that received an e-mail—solicited or unsolicited—from an individual. The Act makes no distinction—even though most Internet users would—between information gathering that is open and obvious (such as a request for mailing address) and that which is largely invisible to the user (such as creating a cookie). All online information gathering “by any means” is covered by the Act.

Finally, the Act is silent on the critical issue of how information collected prior to its effective date (the day following publication of a final implementing rule by the FTC (§ 402)) is to be treated.

Reliance on Notice and Consent

The Act imposes burdensome notice and consent obligations, despite extensive evidence about the ineffectiveness of this approach. Website privacy notices are among the pages least accessed on any website. The experience of the chief privacy officer of Excite@Home, who told an FTC 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 the privacy pages on the company’s website, is typical. Moreover, we know that when Internet users are confronted with “pop-up” notices (whether about license terms or privacy policies), they click through them as rapidly as possible, almost never reading them, in an effort to get on with their browsing.

The FTC reported to Congress in 2000 that 88% of commercial Web sites (100% of the busiest commercial Web sites) had voluntarily posted a privacy policy.² Yet, opinion polls tell us that the rapid growth in the use of privacy notices and their near ubiquity for the past two years has had no effect on the percentage of Internet users expressing concern about the privacy of their information.

The recent experience with the notices required by the Gramm-Leach-Bliley Act's financial privacy provisions illuminate how limited the value is to consumers of notice-and-consent-based privacy protection. As required by that law, by July 1, 2001, 40,000 financial institutions had mailed approximately 4 billion notices. If ever consumers would pay attention and respond, this would appear to be the occasion: The notices came in an avalanche that seems likely to have attracted consumer attention, the press carried a wave of stories about the notices and about state efforts to supplement Gramm-Leach-Bliley's privacy provisions, privacy advocates lauded the opt-out opportunity and offered online services that would write opt-out requests for consumers, and the information at issue—financial information—is among the most sensitive and personal to most individuals.

Yet a late September survey revealed that 35% of the 1001 respondents could not even recall receiving a privacy notice, even though the average American had received 20.³ This has nothing to do with how well written the notices were; the public had ignored the notices so completely that 35% could not even remember getting one. (Not surprisingly, the response rate was negligible. By mid-August, only about 5% of consumers had opted out of having their financial information shared with third parties.)

Before subjecting consumers to another barrage of notices, Congress would do well to learn from its own experience and heed the conclusion of FTC Chairman Timothy Muris:

The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love—until they found out it applied to them.⁴

The Online Personal Privacy Act, however, not merely ignores the record of problems trying to protect privacy with notice-and-consent systems, but promises to exacerbate those problems by requiring three different forms of notice: “clear and conspicuous” notice (§ 102(a)); “robust” notice whenever information is collected (§§ 102(c)-(d)); and a third, unspecified level of

²Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 11 (2000).

³Star Systems, *Financial Privacy: Beyond Title V of Gramm-Leach-Bliley* 9 (2002).

⁴Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Privacy 2001 Conference, Cleveland, OH, Oct. 4, 2001.

notice upon any “material change” in privacy policy, any violation of the Act, or in the event the “security, confidentiality, or integrity” of the information is compromised (§ 103(a)). (The Act also reflects a certain bravado, requiring that “robust notice” be “brief[] and succinct[]” (§ 401(13)). The complexity of legally mandated notices generally reflects the complexity of the law, so if Congress wants a “brief[] and succinct[] notice,” it must impose clear and precise requirements.) Consumers, who already ignore privacy notices whenever possible, are unlikely to know what to do when confronted with this barrage of different, inconsistent notices, and they are unlikely to appreciate the cost that they will ultimately be expected to bear of complying with this cumbersome system.

The Special Problem of Opt-In for “Sensitive” Information

The Act will compel consumers to respond to at least some privacy notices, or punish them if they do not, because it forbids the collection, use, or disclosure of what the Act terms “sensitive” information without “affirmative consent.” This requirement presents many problems, four of which warrant special mention.

First, the phrase “affirmative consent” has no meaning. That is the only form of consent available; “negative consent” is an oxymoron. One might assume from the title of section 102(b) that the drafters meant “opt-in” consent, although neither this term nor “affirmative consent” is defined in the Act.

Second, the Act defines information as “sensitive” by reference only to its content; the Act ignores the context in which the information is collected or used. This is contrary to most U.S. privacy laws, which impose liability for disclosure of information based on the context of the disclosure. It is also contrary to common sense. For example, an individual’s name would in many situations not be considered sensitive, but if included on a list of suspected felons or people who tested positive for HIV, name would be highly sensitive: It is context, not content, that tells us that.

By ignoring this basic point, the Act would treat as “sensitive” information that is voluntarily disclosed (for example, postings to newsgroups in which users express religious beliefs or sexual orientation), and information that is readily perceived (such as race or ethnicity). Irrespective of context, these and other subjects are required to be treated as “sensitive.” This designation is significant because it gives the individual the right to recover statutory damages even where there is no injury (discussed further below).

The requirement that sensitive information be collected, used, or disclosed only with “affirmative consent” also prohibits providers from providing products or services that use “sensitive information” unless the individual can be compelled to read a privacy notice and express “affirmative consent.” The Act thus shifts the burden of acting, and the consequences of not

acting, onto individual data subjects. Previously, they could ignore privacy notices and still enjoy the benefits of online services. Under the Act, they can no longer do so.

Finally, the move to opt-in ignores a growing body of uncontradicted research and experience that shows that opt-in not only burdens and inconveniences consumers, but also is expensive to implement in practice:

- U.S. West found that to obtain opt-in consent to use information about its own customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.) to market services to them cost almost \$30 per customer contacted.⁵
- A 2000 Ernst & Young study of financial institutions representing 30% of financial services industry revenues, found that if financial services companies had to comply with an opt-in law for marketing, they would send out three to six times more direct marketing material, at an additional cost of about \$1 billion per year. The study concluded that the total annual cost to consumers of opt-in's restriction on existing information flows was \$17 billion for the companies studied, or \$56 billion if extrapolated to include the customers of all financial institutions.⁶
- A 2001 study of Australian opt-in laws applicable to credit information concluded that creditors who are constrained by those rules "extend new credit to 11,000 fewer consumers for every 100,000 applicants than would be the case if they were allowed to use the more complete data available under U.S. law."⁷
- A 2002 study by Michael Turner calculates that the annual cost to charities of complying with opt-in privacy laws when fundraising, would be \$16.5 billionC21% of the total amount raised by U.S. charities in 2000.⁸
- Walter Kitchenman has calculated that opt-in could raise the cost of residential mortgages by as much as \$80 billion a year.⁹

⁵Brief for Petitioner and Interveners at 15-16, *U.S. West, Inc. v. Federal Communications Commission*, 182 F.3d 1224, 1239 (10th Cir. 1999), cert. denied 528 U.S. 1188 (2000).

⁶Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies* 16 (2000).

⁷John M. Barron & Michael Staten, *The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience* (2001).

⁸Michael A. Turner & Lawrence G. Buc, *The Impact of Data Restrictions on Fundraising for Charitable & Nonprofit Institutions* 2-3 (2002).

⁹Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns* 7 (1999).

- Robert E. Litan, director of economic studies at The Brookings Institution and a former Deputy Assistant Attorney General of 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.”¹⁰
- The European Union data protection directive conditions the collection, use, or transfer of personal information on opt-in consent, but a January 2001 study by Consumers International found that “[d]espite 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.*”¹¹ Opt-in laws do not appear to have enhanced the confidence of European consumers either.¹² In fact, European data protection officials have acknowledged the impossibility of insisting on opt-in and have instead relied on “implied explicit consent”—what the U.S. calls “opt-out.”

This is not to argue that any of these studies or experiences is directly applicable to the Act, or that opt-in can never work or is never worth the cost, but simply that opt-in imposes often considerable costs which there is no indication the drafters of the Act have taken into account. In fact, quite the contrary. The Act asserts in finding 17 that costs are irrelevant because however great they are, they are worth it: “Whatever costs may be borne by industry will be significantly offset by the economic benefits to the commercial Internet created by increased consumer confidence occasioned by greater privacy protection.” The only problem, is that all of the available data are to the contrary. The research shows, in the words of Alabama Attorney General Bill Pryor, that when opt-in laws are adopted, consumers “pay the price in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace.”¹³

The Problem of Consumer Contact

The Act exacerbates the problems inherent in requiring notice and conditioning information flows on opt-in consent by applying these provisions even where the provider or operator has collected no contact information. The Act requires notice upon any “material change” in privacy policy, any violation of the Act, or in the event the “security, confidentiality, or

¹⁰Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, AEI-Brookings Joint Center for Regulatory Studies Working Paper 99-3 at 11 (1999).

¹¹Consumers International, *Privacy@net: An International Comparative Study of Consumer Privacy on the Internet* at 6 (2001) (emphasis added).

¹²*IBM Multi-National Consumer Privacy Survey* at 22 (1999).

¹³Bill Pryor, *Protecting Privacy: Some First Principles*, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, DC, at 4.

integrity” of the information is compromised (§ 103(a)). The drafters obviously assumed that all information collected would include contact information, however, the Act applies to many forms of data other than contact information. So if, for example, a website places a cookie on a users’ website (which is specifically covered by the bill), and later decides not to use cookies, how is the site to notify all of its users? It doesn’t have e-mail addresses or a list of computers with cookies it has placed there. The only way a website could comply with the Act is to collect even more information—an ironic result for a “Personal Privacy Act.”

Because of vague and broad drafting, the occasions on which this problem will arise are likely to be numerous. Recall that a provider or operator has to provide notice to every person affected if the “security, confidentiality, or integrity of such information is compromised . . . by any act or failure to act of the provider or operator.” (§ 103(b)(1)(B)) What does it mean to “compromise” the “security, confidentiality, or integrity” of information and what, if anything, does the phrase “act or failure to act” exclude? Providers are likely to constantly face the obligation to contact individual users—an expensive and burdensome process in any event, and one that many consumers seem unlikely to appreciate. The expense and burden are only exacerbated by requiring contact with people for whom the provider or operator has collected no contact information.

Access and Correction

The Act requires internet service and online service providers and operators of commercial websites to provide data subjects with access to information about them and an opportunity to “suggest a correction or deletion” of that information (§ 105). This is a very troubling provision, because of the substantial risks it creates for individuals. Many of these risks were highlighted by the FTC’s Advisory Committee on Online Access and Security (“Advisory Committee”). One of the most important, as the Advisory Committee noted, is the “very real tension between access and security”:

Unlike the other Fair Information Practice principles, the access principle sometimes pits privacy against privacy. . . . [P]rivacy is lost if a security failure results in access being granted to the wrong person—an investigator making a pretext call, a con man engaged in identity theft, or, in some instances, one family member in conflict with another.¹⁴

The problem is how to provide access without “running the risk that others will also gain access to that data.” To date, this has proved very difficult, especially online. The breadth of information to which the Act applies only compounds this difficulty. If a user provides a website with his or her name and address to enter a contest or request a brochure, and later wishes to access that information, how does the website know that the person requesting access is the same

¹⁴*Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security* at 15 (2000), reprinted as an appendix to *Privacy Online*, supra.

person who provided the information? Yet the risk of providing access to, and an opportunity to correct, one individual's personal information to another individual is significant; access would then become the perfect tool for identity theft, and the government that mandates access the unwitting accomplice of identity thieves. "Giving access to the wrong person could turn a privacy policy into an anti-privacy policy."¹⁵

To date, virtually all of the measures currently available for authenticating identity require that the individual provide more information about himself or herself. To maintain the necessary authentication tools, providers will likely have to seek and store more personal information, such as Social Security Number or mother's maiden name, or require the user to create an account.

Because the Act is so broad, it requires the centralization of disparate pieces of information collected from users, so that a provider or operator can respond to an access request. The extent of this problem is difficult to predict because of the Act's vagueness, but, for example, the Act appears to apply to usage logs and back-up tapes, which usually contain information about individual users. Although these sources are normally used only in the event of a system failure, a dispute regarding a transaction, or, in the aggregate, to monitor and enhance system performance, the Act would appear to require providers to bring together all of this information, together with all of the other information collected about an individual—to engage in the very act of "profiling" and the creation of super database that privacy principles traditionally argue against.

In fact, the Act requires that access be provided to all of the information "collected" about an individual user. There is no reference to whether or not that information has been stored. Do the drafters therefore intend to require providers to store information they would otherwise discard so that they can provide access to it at a later date? Similarly, the Act explicitly covers "cookies"—small data files stored on individual users' computers. How are providers going to provide users with access to these files that the users—not the providers—possess?

After studying these "complicated" and "controversial" issues in detail for months, the FTC Advisory Committee could not reach any consensus on whether or how access should be provided. The imprecision of the Act's access provisions suggest that the drafters have not yet resolved these issues either. This may explain why they included a provision eliminating liability, not only under this Act but under all federal and state law, for harms caused by providers trying to comply with the Act's access provisions. Given the many issues surrounding access, and the potentially profound consequences of errors, this only seems fair to providers. But it will be of little comfort to individual Internet users whose privacy is invaded or identity stolen as a result of this federal access mandate.

Finally, the Act requires that users be given a "reasonable opportunity" to "suggest a correction or deletion" of information collected online (§ 105(a)(2)). Providers must "make the

¹⁵Id. at 4.

correction a part of that user's . . . information . . . or make the deletion, for all future disclosures and other use purposes" (§ 105(a)(3)) If the provider declines, it must comply with procedures requiring notice in writing to the data subject justifying what the suggested change is "inaccurate or otherwise inappropriate" and providing a "reasonable opportunity for the user to refute" those reasons (§ 105(b)). These terms are vague and ambiguous—the word "reasonable" or "reasonably" appears on average at least once in every paragraph, eight times in the Access section alone. The requirement that the correction or deletion suggestion be attached to future "disclosures and other use purposes" is not only unclear, it also ignores the practical reality of the online environment. In practice, information is copied and combined and distributed in many different ways. Appending corrections or making deletions is not always practical, nor do they always have any effect. These provisions and their lack of clarity increase the difficulty and cost of compliance and increase the risk that consumers will be injured through access errors.

Enforcement

The Act's enforcement provisions are particularly problematic because they put in place a bureaucratic, expensive, and duplicative enforcement system, the breadth and complexity of which is exacerbated by ambiguous language. A single alleged violation of the Act can subject a provider or operator to suits by the FTC, 51 state attorneys general, and private individuals. The Act purports to limit the states—but not private parties—by providing that states may not institute actions where the Commission has already brought a suit, but it applies this provision to state actions brought under this Act, so states are free to bring suits—as they have been doing vigorously—under other state and federal laws (§ 204(d)). Pile-on litigation imposes significant costs without achieving any additional benefits; the sections of this Act permitting it reflect a serious flaw.

The Act creates a private right of action for violations involving sensitive information, even if the plaintiffs suffer no harm or injury. The action is a strict liability offense: It does not matter how responsibly the provider or operator has behaved, if any of its actions involving sensitive information violate the Act, the provider or operator is liable to all of its users. If there is "actual harm"—another key term that is not defined—then individuals are entitled to the greater of "actual monetary loss" or \$5,000 (§ 203(a)). Depending upon how "actual harm" is interpreted by courts (for example, does it include emotional distress or the cost of a stamp or telephone call?), this provision is likely to result in overcompensating some individuals at the cost of others who will pay the price in terms of higher prices or reduced service.

The risk here is considerable, because of the breadth of the Act and the volume of Internet data. Providers can easily collect data on millions of users in a single day. A single error, or a good faith practice with which a court later disagrees, can subject the provider or operator to pay \$5,000 to every user whose sensitive data was affected. These provisions are a gift to the plaintiffs bar and class action attorneys, but seriously threaten the livelihood of many providers of internet and online services and operators of commercial websites.

The vagueness of the enforcement provisions is also likely to impose additional unnecessary costs. For example, section 202(a) designates a violation of this Act an “unfair or deceptive act.” Which is it? There is a significant legal distinction between the Commission’s authority to remedy “deceptive” acts, under which the FTC has successfully proceeded against dozens of website operators for failing to adhere to their published privacy policies, and the Commission’s authority with regard to “unfair” acts.

Similarly, section 202(c) provides that a violation of this Act shall be “deemed to be a violation of a requirement imposed under that Act,” referring to five other acts that give other regulatory agencies their powers. What requirement is violated and under which act? Congressional ambiguity on these important issues will only lead to inconsistency, uncertainty, and unnecessary expense in enforcement.

Section 202(e) sets up a complicated civil fine distribution mechanism. The FTC must, with regard to every civil penalty it collects for violations of the Act involving “nonsensitive” information, create procedures to distribute the proceeds to people who file claims claiming “loss or damage” (§ 202(e)(2)). (Ironically, “loss or damage” is not required for filing a private civil suit, but is for filing a claim with the FTC.) In each case, the FTC must hold the money for “not less than 180 days,” and cannot distribute more than \$200 to any one individual, irrespective of how much he or she may have been harmed. These requirements promise to further whittle away the government and private resources available for preventing, rectifying, and compensating victims of real privacy harms.

Exceptions and the Lack of Uniformity

The Act provides an array of exceptions. One of the most significant is the exclusion of noncommercial websites. Why impose such a variety of burdensome requirements on commercial websites, the vast majority of which operate in a competitive market and, according to the FTC, have voluntarily posted privacy policies, but exclude noncommercial websites, which by definition operate outside of the competition provided by commercial markets? Is the failure to provide notice or access more serious when committed by a business than by a charity, advocacy group, alumni association, or political party?

Similarly, the Act wisely extends its provisions to the Senate and federal agencies, but omits the House of Representative and state and local governments. A September 2000 Brown University study of 1,700 state and local government websites found that only 7% posted a privacy policy,¹⁶ at the same time that the FTC found that 88% of commercial websites (100% of

¹⁶Darrell M. West, *Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments* (Sept. 2000).

the busiest commercial websites) had voluntarily posted a privacy policy.¹⁷ It is difficult to imagine why the Act then applies to only commercial, Senate, and federal agency sites.

One final and poignant example of the Act's inconsistency is its troubling treatment of government access to data. The central and oldest privacy protection in the United States is the Fourth Amendment's prohibition against government invasion of privacy. The Act, however, appears to weaken that protection by allowing disclosure to law enforcement, without any of the Act's privacy protections, upon mere "request or demand" (§ 104(c)(1)(A)). And while the Act requires court orders that mandate disclosure to include "appropriate safeguards" against "unauthorized disclosure," there is no similar requirement applicable to law enforcement when it obtains information through request or demand (§104(c)(2)).

Constitutionality

The Act imposes significant limits on the collection and use of information for expression and therefore must be reviewed under the First Amendment. The breadth of the Act and the lack of precision in its drafting heighten constitutional concerns.

Under the First Amendment, the government bears the burden of demonstrating that the Act serves a public interest that is "substantial," that the Act "advances these interests in a direct and material way," and that "the extent of the restriction on protected speech is in reasonable proportion to the interests served."¹⁸ The government cannot satisfy this heavy burden "by mere speculation or conjecture."¹⁹ Instead, the government must show that the "the harms it recites are real and that its restriction will in fact alleviate them to a material degree."²⁰ This requires a "careful calculat[ion of] the costs and benefits associated with the burden on speech imposed by its prohibition."²¹

As drafted, this Act is unlikely to withstand constitutional review. It applies to information that poses no threat of harm to individuals, and allows suits by individuals who have suffered no harm. It conditions speech on conditions that are burdensome and in some cases impossible. Many of its provisions impose unnecessary costs or are so vague as to be unclear as to what they require. Yet the Act appears wholly unconcerned with the costs of its requirements to either consumers or businesses. It ignores the growing volume of uncontroverted evidence about the ineffectiveness and expense of notice-and-consent-based privacy restrictions, noting only that "[w]hatever [the] costs," they "will be significantly offset by the economic benefits to the

¹⁷*Privacy Online*, supra, at 11.

¹⁸*Edenfield v. Fane*, 507 U.S. 761, 767 (1993).

¹⁹*Id.* at 770-71 (citations omitted).

²⁰*Id.*

²¹*City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993) (quotation omitted).

commercial Internet created by increased consumer confidence occasioned by greater privacy protection” (finding 17).

The Act requires opt-in consent, despite the special burdens it imposes, without any showing that opt-out consent or some other mechanism would be satisfactory. Yet the Supreme Court has struck down many ordinances that would require affirmative consent before receiving door-to-door solicitations,²² before receiving Communist literature,²³ even before receiving “patently offensive” cable programming.²⁴

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 rules of the Federal Communications Commission (“FCC”) 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.²⁵ 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.”²⁶ 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. Because the government could not bear this burden, the court struck down the rules as unconstitutional.

Conclusion

The Online Personal Privacy Act has many problems. Some of those are inherent in the Act’s substantive approach to privacy. Despite the Act’s finding that consumer fears about privacy are causing them to avoid conducting commerce online, research data demonstrate that individuals are flocking to the Internet. The number making purchases online is increasing 45% per year.²⁷ Many of the features that attract consumers to the Internet depend on the ability to collect and use information productively. Eliminating these conveniences, or conditioning them on

²²*Martin v. Struthers*, 319 U.S. 141 (1943).

²³*Lamont v. Postmaster General*, 381 U.S. 301 (1965).

²⁴*Denver Area Educational Telecommunications Consortium, Inc. v. Federal Communications Commission*, 518 U.S. 727 (1996).

²⁵*U.S. West*, 182 F.3d at 1235.

²⁶*Id.* at 1235 (quoting *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 486 (1995)).

²⁷Pew Internet & American Life Project, *Getting Serious Online: As Americans Gain Experience, They Use the Web More at Work, Write Emails with More Significant Content, Perform More Online Transactions, and Pursue More Serious Activities* (2002).

repetitive, intrusive privacy notices, will not serve consumer interests, and could easily undermine many services and products that the public values. Free access to content requires that online companies tightly control expenses and seek to generate revenue through alternative routes. The use of information is often critical to both efforts, and Congress should think carefully before enacting a law that threatens the viability of free access to Internet content. However, reasonable minds may differ about these issues: Clearly, some people believe that it is better to restrict access to the Internet or the availability of products and services there, rather than allow information to be used freely, constrained only by laws prohibiting harmful and deceptive uses and market-driven privacy policies providing other protections.

Many of the Act's most significant problems, however, are the result of poor drafting and a failure to think through how the Act will be applied in practice. In particular, the Act's complexity and its reliance on vague and undefined terms undermine the Act's effectiveness, add to its cost, and increase the likelihood that it will be found unconstitutional. These drafting failures have no champions: They harm consumers and businesses without achieving any benefits. They make the Act, as currently drafted, untenable.