

Statement of John C. Dugan, Partner, Covington & Burling

on behalf of the

Financial Services Coordinating Council

(American Bankers Association)

(American Council of Life Insurers)

(American Insurance Association)

(Securities Industry Association)

Testimony Before the U.S. Senate Committee on
Commerce, Science, and Transportation

Hearing on S.2201, the “Online Personal Privacy Act”

April 25, 2002

My name is John Dugan, and I am a partner with the law firm of Covington & Burling. I am testifying today on behalf of the Financial Services Coordinating Council (“FSCC”), whose members include the American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry Association. These organizations represent thousands of large and small banks, insurance companies, and securities firms that, taken together, provide financial services to virtually every household in America.

The FSCC appreciates the opportunity to testify before this subcommittee on S.2201, the Online Personal Privacy Act. We are keenly aware of the need to maintain the privacy of personal information. With the enactment of the Gramm-Leach-Bliley Act in 1999 (the “GLB Act”), thousands of financial institutions across the country have expended enormous amounts of time, energy, and resources to provide financial institution customers with comprehensive privacy protections. Coupled with the protections mandated by the Fair Credit Reporting Act, these consumers now must be provided--

- **Notice** of the institution’s practices regarding information collection, disclosure, and use, which must be clear, conspicuous, and updated each year;
- **Opt-Out Choice** regarding the institution’s sharing of information with nonaffiliated third parties, and in certain instances, with affiliates;
- **Security** in the form of mandatory policies, procedures, systems and controls to ensure that personal information remains confidential; and
- **Enforcement** of privacy protections via the full panoply of enforcement powers of the agencies that regulate financial institutions, *i.e.*, the federal bank regulators, the Securities and Exchange Commission, state insurance authorities, and the Federal Trade Commission.

In addition to these protections, customers of financial institutions that handle personal health information receive the extensive privacy protections of federal and state medical privacy laws. All of these mandatory privacy protections apply equally to financial institution consumers in both the offline and online contexts. Taken together, they form perhaps the most comprehensive set of mandatory privacy protections in the country. The proposed requirements of S.2201 would apply to financial institutions on top of this extensive privacy regime.

The FSCC strongly opposes S.2201 bill for the following reasons. *First*, financial institutions are subject already to the comprehensive privacy regulation described above, which Congress carefully debated and enacted less than three years ago; it would be both unnecessary and costly to subject them to the new and conflicting restrictions included in S.2201. *Second*, the bill will thwart the development of e-commerce by, for example, imposing dual and conflicting privacy standards for companies that collect information both online and offline, often from the same customer. *Third*, parts of the bill apply much more restrictively to financial institutions, because of the nature of their business, than they do to other types of companies -- even though financial institutions are already subject to extensive privacy regulation. *Fourth*, a number of the bill's provisions are simply far too restrictive. *Finally*, the FSCC believes that the bill's heavy regulatory approach is unnecessary in view of the increasingly effective self-regulatory efforts of the online industry, including through new technologies.

I. Financial Institutions and their Customers Don't Need Yet Another Set of Privacy Rules

S.2201 seems to be aimed primarily at online businesses and advertisers that are not now subject to mandatory privacy regulation. But the bill sweeps in any business that deals with any consumer via the Internet, which means that privacy-regulated businesses like financial institutions are included as well. Because of the financial institution privacy protections described above, which are already in place and apply in the online context, the FSCC believes that the bill's application to financial institutions is unnecessary.

Just over two years ago, Congress carefully considered the costs and benefits of the privacy-related restrictions that ought to apply to financial institutions and their consumers, which resulted in Title V of the GLB Act. Financial regulators subsequently implemented detailed privacy regulations for the first time, and financial institutions have spent many millions of dollars to build systems to comply and protect customer information. Financial institution customers now enjoy the benefit of those protections, which ought to be given a chance to work.

Moreover, S.2201 would subject financial institutions to a whole new layer of privacy regulations that would apply at the same time as those imposed by the GLB Act and other financial privacy laws. That would mean two types of notices to customers, two types of consent provisions, redundant security requirements, and two distinct types of enforcement regimes. This is far too burdensome and costly. It could also confuse customers, which in turn would result in conflicting instructions by consumers to their

financial institutions (*e.g.*, opt-out in one context, opt-in in another). Financial institutions should be subject to a single privacy regime that applies equally in all contexts.

II. S.2201 Will Thwart the Development of Electronic Commerce

The Internet is bringing enormous social and economic benefits to its users and to nations around the world. It is empowering individuals to seek, receive, and share information and ideas. It is changing how we educate, shop, spend our time, and transact business. And, perhaps most importantly, it is equalizing access to information, giving everyone with a computer and an Internet connection an opportunity both to acquire and use information more effectively.

Throughout its short history, the Internet has been a virtually regulation-free environment. In the United States, regulations affecting the privacy of information online have been limited to only those necessary to protect our most vulnerable online population—children. Because of this philosophy of regulatory restraint, electronic commerce has thrived. According to a recent U.S. Department of Commerce survey, more than half of Americans are using the Internet and among these Internet users, 39 percent of them are making online purchases.

While the European Union has adopted comprehensive privacy regulations, the United States has avoided such an approach. On numerous occasions, government officials have appropriately voiced concern over problems inherent with applying old legislative paradigms to the constantly changing Internet. These concerns appropriately

recognize (1) that market-driven solutions to online problems provide the most effective means to ensure the continued growth of the Internet, and (2) that any governmental regulation should target discrete concerns and be carefully tailored to reach no broader than necessary in order to solve the problem at hand. The Children's Online Privacy Protection Act ("COPPA") and the Electronic Signatures in Globalization Act ("E-SIGN") reflect this balanced approach. Both laws are narrowly tailored to target specific online concerns and provide a workable legal framework within which these concerns can be resolved.

S.2201 is a marked departure from this philosophy of restraint and targeted governmental action. The bill treats information collected online differently than information collected by other means and thereby subjects the vast majority of U.S. companies to two substantially different privacy regimes in the offline and online environments. In practice, this approach will retard the use of online channels, or, at the very least, require a company to adhere to the bill's substantive requirements with respect to all of its information collection activities.

Today, companies like financial institutions frequently operate according to a "clicks and bricks" business model under which customer relationships begin offline and migrate online. Specifically, a company collects personal information about a consumer offline when it begins a relationship with a consumer and then again online when the consumer, on his own or through the prompting of the company, uses the company's services over the Internet. In many cases, the information collected online is exactly the same as that collected offline (i.e., name, address, account number), but in other cases the

information may be different. As a result, it is fairly typical that a company has one database that includes both personal information initially collected non-electronically (and subsequently entered into a computer) and similar or different information collected over the Internet.

S.2201 would severely impair a company's ability to operate under this "clicks and bricks" business model. Such a company would be forced to maintain two separate information systems—an offline system subject to any applicable offline privacy regulations (such as the GLB Act or healthcare privacy rules) and an online system subject to *both* those privacy requirements and the requirements contained in S.2201. In many cases the two systems would apply to personal information collected from the same individual. Such a two-tiered system would be extremely costly and burdensome to manage. And it could cause some companies, especially smaller ones, to avoid online operations altogether.

III. S.2201 Will Have a Disproportionate Impact on Financial Institutions

S.2201 creates two categories of personally identifiable information—"sensitive" and "non-sensitive"—and regulates sensitive information much more stringently than non-sensitive information. The bill requires online operators to obtain *opt-in* consent before they collect, disclose, or otherwise use *sensitive* information, and would use a private right of action and class actions to address violations of such requirements. In contrast, with respect to *non-sensitive* information, the bill requires only *opt-out* consent and establishes no express private right of action for individuals.

For most types of businesses, the increased restrictions on “sensitive” information present relatively few additional problems, because “sensitive information” does not constitute the core of their business. That is not the case with financial institutions. S.2201 defines “sensitive personally identifiable information” to include “sensitive financial information,” and that term includes the amount of income earned or losses suffered by an individual; balance “information” regarding any financial services account; any insurance policy information; and outstanding credit card, debt, or loan obligations. Although such information may be incidental to the operations of many online companies, it frequently is *the* business of banks, insurance companies, and securities firms.

For example, an online clothing retailer might want to provide special discount coupons to its best customers, who might be those individuals who purchased more than a certain amount of clothing each year. The retailer’s discount offer would be subject to the bill’s opt-out requirement, and a violation of the requirement would not be subject to a private right of action or class action enforcement. In contrast, a bank might want to give its biggest depositors a discount on unrelated financial services such as an insurance product or a loan. Or an insurance company might want to reward a large term-life insurance policyholder with a discount on his or her car insurance. In these cases, the discount offers would be subject to the bill’s opt-*in* requirement, and any related violations of the statute would be subject to (and a target for) class action enforcement.

Thus, financial institutions, which are subject to much more comprehensive privacy regulation than other online businesses, are perversely subject to the bill’s most

onerous restrictions with respect to their core businesses, while less regulated online providers are not. As discussed below, it would be extremely costly and unfair to target financial institutions with some of the bill's most restrictive provisions, *i.e.*, the opt-in and private right of action, which also have particularly negative effects on financial institutions that handle health information.

A. S.2201's "opt-in" requirement will effectively prohibit core financial institution practices that benefit consumers.

Financial institutions are well aware of the unique position of responsibility they have regarding an individual's personal information, including health information. The member companies of the trade groups belonging to the FSCC are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that these companies have an obligation to assure individuals of the confidentiality of that information.

However, the FSCC strongly opposes S.2201's opt-in requirement, especially when it is coupled with the bill's unrelated *use* requirement. That is, unlike the GLB Act, which applies only to *disclosures* of personal information by a financial institution to third parties, S.2201 also restricts virtually any *use* of personal information by the institution itself, even if the information were not disclosed to others and were used to benefit the customer. This would constitute a new and unnecessary roadblock between all companies and their customers.

The combination of the opt-in and unrelated use restrictions would require financial institutions to contact customers and obtain their prior permission to engage in core business activities involving personal information – which in practice would constitute a *de facto* prohibition on responsible information sharing that benefits consumers. Not even Europe’s Privacy Directive, which on paper is one the most stringent privacy regimes, goes this far. Instead, the EU Directive permits entities to follow an opt-out approach with respect to the use and disclosure of financial information.

The FSCC believes that there is a fundamental flaw with the way opt-in requirements work. Such provisions deprive consumers of benefits from information sharing, such as discounts on other types of financial products. In essence, an opt-in creates a “default rule” that stops the free flow of information (which is especially critical to Internet transactions). This in turn makes the provision of financial services more expensive and reduces the products and services that can be offered. Further, consumers rarely exercise opt-in consent of any kind—even those consumers who would want to receive the benefits of information sharing if they knew about them. In contrast, a *meaningful* opt-out gives privacy-sensitive consumers as much choice as an opt-in, but without setting the default rule to deny benefits to consumers who are less privacy-sensitive.

B. S.2201's narrow exceptions to the bill's opt-in (and opt-out) will prevent critical information sharing by financial institutions.

Privacy regimes that impose customer consent restrictions on financial institutions nearly always include a range of specific exceptions. These exceptions cover circumstances in which consent is either implied, unnecessary, or would impede a legitimate public policy goal. For example, the Gramm-Leach-Bliley Act and its implementing regulations at both the federal and state level recognize well over 30 such exceptions, which are critically important to financial institutions doing business with their customers. Such “doing business” exceptions, which have never been controversial, permit disclosures that are necessary, for example, to prevent fraud, create credit histories, underwrite insurance, engage in risk management practices, securitize loans, outsource functions to agents, obtain legal advice, etc.

In contrast, S.2201 includes only four exceptions to the bill's opt-in and opt-out requirements. Section 104's exceptions apply to certain information collection, use, and disclosure practices that are necessary to (1) protect the security or integrity of the website; (2) conduct a transaction, deliver a product, or complete an arrangement for which personal information has been provided; (3) provide other products or services that are “integrally related” to the transaction, service, product, or arrangement for which the consumer provided the information; and (4) to comply with law enforcement or a judicial process.

These provisions, although vague, were clearly crafted to reach services provided in the context of completing online retail sales. Yet financial institutions necessarily do much more with online information than engage in marketing or the other extremely narrow range of activities covered by the bill's exceptions. The combination of the opt-in and unrelated use provisions could potentially shut down core business use and sharing practices, including sharing information with credit bureaus, securitizing mortgages, running normal credit card operations, and engaging in a range of activities related to insurance underwriting. It is unlikely that these activities would qualify as "necessary to conduct" or "integrally related" to the transaction, service, or product obtained by the consumer. This would have the unintended, negative consequence of disadvantaging, rather than helping, consumers.

C. The private-right-of-action provision will invite abusive class action litigation against financial institutions.

Under the bill's private right of action, *any* showing of actual harm involving sensitive information, however small, will provide a plaintiff with a guaranteed recovery of at least \$5,000 per violation. Such a provision is clearly intended to attract class action litigation as an enforcement mechanism. Because financial institutions' core business involves information that the bill deems "sensitive," the bill would make them the new target of choice for the plaintiffs' bar.

This is both unfair and unnecessary. Unlike most online businesses, financial institutions are already heavily regulated, and their regulators have broad powers to punish violations of law – which they do not hesitate to exercise. That is why, in the

privacy context, Congress chose not to authorize a private right of action or class actions as a means to enforce the GLB Act's privacy provisions. Instead, enforcement is accomplished through the full panoply of enforcement powers of the relevant financial regulator, *e.g.*, federal banking agencies for banks; the SEC for securities firms; state insurance authorities for insurance companies; and the FTC for non-traditional "financial institutions." This enforcement regime works. The FSCC therefore strongly opposes the creation of a new class action mechanism that, while having little impact on most online businesses, would create a huge and unnecessary new source of litigation cost for financial institutions.

D. The bill will have a disproportionate impact on financial institutions that handle health information.

S.2201 includes individually identifiable health information within the definition of sensitive information that is subject to the bill's stricter opt-in requirements. This ignores the complex and detailed issues surrounding the protection of health information. Financial institutions, particularly insurance companies, must be able to disclose or otherwise use personally identifiable health information to perform essential, legitimate insurance business functions, such as underwriting and claims evaluations. In addition, insurers must be able to disclose and use personally identifiable health information to perform important business functions that are not necessarily directly related to a particular insurance contract but that are essential to the administration or servicing of *insurance policies generally*, such as, for example, developing and maintaining of computer systems. An opt-in that would jeopardize these uses and disclosures of

personally identifiable health information would also jeopardize insurers' ability to serve and fulfill their contractual obligations to existing and prospective customers.

Insurers also must regularly disclose personal health and financial information to:

- (1) state insurance departments as a result of their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers;
- (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), which imposes and monitors adherence to requirements with respect to member insurers' conduct in the marketplace; and
- (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations that typically require broad access to policyholder information.

In addition, insurers need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made *not only* to law enforcement agencies, but also to state insurance departments, the Medical Information Bureau (MIB), or outside attorneys or investigators, who work for the insurer. To the extent that S.2201's opt-in would limit these disclosures, it would undermine the public policy reason for making them—to protect consumers.

Existing federal and state privacy regimes, including the final Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) promulgated by the Department of Health and Human Services as required by the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191), provide fundamental protections to the privacy of health information. Unlike S.2201, the HIPAA Privacy Rule

includes a variety of carefully considered exceptions to its authorization requirement in order to strike a proper balance between the legitimate expectations of consumers concerning the treatment of their information and the ability of insurers and others to use personal health information responsibly. Also, many state laws and regulations, particularly those adopted recently to implement the privacy requirements of the GLB Act, contain sections specifically addressing the confidentiality of health information and specifically providing exceptions to their opt-in requirements applicable to disclosures of health information.

In short, the issue of health information privacy is difficult and complex. It is, at best, unclear how the health provisions of S.2201 compare and/or integrate with existing laws and what impact this legislation will have on financial institutions. At worst, the combination of the opt-in and class action enforcement could have extremely negative consequences.

IV. Other Concerns with S.2201

There are a number of other fundamental problems with the provisions of S.2201 that are not unique to financial institutions.

“Use” Restrictions. The problem with the bill’s blanket restriction on unrelated “uses” of information is not limited to sensitive information covered by the opt-in. It also applies to nonsensitive information covered by the opt-out. (A business may not disclose or “otherwise use” information collected online without notice and opt-out.) Among other things, this will impair a business from engaging in generally accepted marketing

activities *with its own customers*, and a charity from soliciting contributors for additional contributions. Thus, the FSCC believes the use restriction is both unnecessary and overly broad.

Access. S.2201 will impose access requirements that will be extremely costly and that will reduce security on the Internet. S.2201 subjects access requests to a vague reasonableness test and fails to exclude information, such as trade secrets or internal operating procedures, to which consumers should never have access. In addition, S.2201 fails to recognize that information may not be maintained in centralized databases searchable by customer name. (And privacy advocates have long advocated that businesses should *not* be encouraged to establish such centralized databases because of increased possibilities for obtaining and using too much information about an individual too easily.) Even where databases are highly centralized, the costs of complying with this requirement will far exceed the nominal charges permitted under the bill. S.2201 also fails to define what it means to “delete” a record in an electronic environment. For example, must all back-up tapes be retrieved from storage and searched for relevant records when a “delete” request is received? What about requests to delete personal information when there is a legal obligation or important business reason to retain such information? The bill does not provide guidance on these important questions.

Financial institutions already provide their customers—often in real time—with access to the personal information of greatest concern to them, *i.e.*, their account balances and transaction statements. In addition, the Fair Credit Reporting Act provides consumers with extensive access and correction rights regarding financial institution

information that is used to make very significant decisions about them, *i.e.*, to grant or deny credit or insurance. For these reasons, there is no need to impose an additional and vague access requirement that can be used for “fishing expeditions” to search for violations of the Act – especially when violations can be easily translated into class action litigation.

Security. S.2201 contains security requirements that duplicate those already established for financial institutions in the GLB Act. Specifically, the GLB Act and its implementing regulations require that each financial institution protect the security and confidentiality of customers’ nonpublic personal information and implement a comprehensive security program. The differences between the security provisions of S.2201 and the GLB Act will lead to unnecessary increased costs to ensure that security procedures meet multiple sets of requirements.

V. S.2201 Is Unnecessary Because Private Sector Efforts Are Working

Finally, apart from the fact that financial institutions are already subject to comprehensive privacy regulation, the FSCC believes that the private sector has taken and continues to take significant steps to address online privacy concerns. These efforts are particularly well suited for solving privacy-related problems on the Internet. This is so because private sector initiatives generally can respond more quickly than legislative solutions to changing technologies and evolving online business and social practices. In addition, private-sector mechanisms, because they are consumer driven by nature, are more likely to permit users to choose among various solutions based on their individual

privacy preferences and thereby avoid the problem of over- and under-breadth that is unavoidable in government regulation, which typically must be one dimensional in nature.

Recent surveys indicate that the private sector's efforts at self-regulation are working. For example, the *Privacy Online* report released earlier this year by the Progress and Freedom Foundation shows that nearly all of the most popular websites (99%) and the vast majority of randomly sampled websites (80%, up from 64% in 2000) post some form of privacy notice if they collect personally identifiable information. Of those websites collecting personally identifiable information, 71% of randomly sampled sites and 89% of the most popular sites offer consumers some form of choice with respect to disclosing that information internally, and almost all (93% up from 77% last year) of the most popular sites and the majority of randomly sampled sites (65%) offer consumers choice over disclosures to third parties. Finally, the survey showed that websites are increasingly likely to tell consumers that they are taking adequate security measures to protect collected information.

In addition, website operators continue to seek certification under seal programs such as TRUSTe and BBBOnline. By the end of 2001, TRUSTe had certified more than 2000 websites in a variety of industries (up from roughly 500 websites in 1999) and BBBOnline has certified more than 760 sites, up from 450 two years ago. The FTC has recognized that such seal programs are an effective method for delivering privacy protections to consumers. In particular, the FTC has endorsed seal programs as a means of complying with the provisions of COPPA—the FTC has created a safe harbor so that

websites that comply with, for example, TRUSTe's children's privacy seal, will be deemed to be in compliance with COPPA as well.

In addition to these efforts, technology provides compelling solutions to many online privacy concerns. For example, P3P, a privacy-enhancing technology that enables users to specify a level of privacy protection based on a website's practices for tracking data, is continuing to gain acceptance and prominence as an effective method of protecting consumers' online privacy. Among the most popular websites, 23% have implemented P3P, and Internet Explorer 6 includes the P3P function.

In sum, like the Federal Trade Commission, the FSCC believes that the significant and evolving steps taken by the private sector to address online privacy concerns makes additional governmental regulation unnecessary at this time, including S.2201.
