The Policy Aspect, Consumer Data Privacy

Clyde Mitchell∗ Carl Howard† Oliver I. Ireland‡
Joel R. Reidenberg** Jay N. Soloway††

Copyright ©2000 by the authors.  Fordham Journal of Corporate & Financial Law is produced by The Berkeley Electronic Press (bepress).  http://ir.lawnet.fordham.edu/jcfl
MR. MITCHELL: Let's get started. My name is Clyde Mitchell. This is the Consumer Data Privacy panel.

I think that data privacy is one of the aspects of Gramm-Leach-Bliley in which, it seems to me, we all have two interests. We are all consumers. How does it affect us as consumers, and how does data privacy regulation affect us from a professional standpoint? It will be interesting to see the positions of the various panelists and how the story unfolds.

As most of you are aware, I am sure, the privacy issues in Gramm-Leach-Bliley came into play pretty late in the process. I am not an expert in this area and a number of things are confusing to me.

For example, I think we heard Chairman Leach say this

---

* Adjunct Professor, Fordham University School of Law.
** Vice President & Associate General Counsel, Bank Regulation, Citigroup.
*** Associate General Counsel, Board of Governors of the Federal Reserve System.
**** Professor, Fordham University School of Law.
***** Senior Vice President and Associate General Counsel, Chase Manhattan Bank.

morning,³ and other legislators have commented also, that Gramm-Leach-Bliley contains one of the most comprehensive packages for privacy protection. On the other side, Senator Shelby and others have described this same package as “a sham.”⁴ These positions are pretty diametrically opposed. Are both accurate? Is one correct? Is one not correct?

A number of state legislators, financial services officials and trade association executives suggest giving Gramm-Leach-Bliley a chance to work,⁵ proposing, “Let’s see how the industry and consumers are affected by it. Let it play out before we do anything else.”

On the other hand, at the federal level and at the state level, what are being suggested are tougher privacy provisions.⁶ I think there is legislation moving through Congress⁷ and in twenty-two

---

⁴. Dean Anason, Minn., N.Y. Vow to Keep Prosecuting Privacy Cases, AM. BANKER, Mar. 24, 2000, at 1; see also Clyde Mitchell, Privacy and Gramm-Leach-Bliley’s Financial Services Modernization, N.Y. L.J., Apr. 19, 2000, at 3 (noting that a Congressional Privacy Caucus was established by U.S. senators and representatives in February 2000, to “close the loopholes created by” Gramm-Leach-Bliley).
⁶. See Kirk Nahra, Tick Tock: The GLB Countdown Continues, METROPOLITAN CORP. Couns., Dec. 2000, at 7 [hereinafter Nahra] (“Already, immediately following the November elections, there are reports of privacy emerging as a ‘first tier’ issue in Congress next year, with predictions by congressional insiders that ‘lawmakers generally agree that medical and financial information must be protected more securely than current law mandates.’”).
⁷. See e.g., S 324 Social Security Number Privacy Act of 2001 (a bill proposed by Senator Richard C. Shelby (R-AL), intended to amend the Gramm-Leach-Bliley Act by prohibiting the sale of social security numbers by financial institutions); S 450 Financial Institution Privacy Protection Act of 2000 (a bill
state legislatures to do that. I guess the biggest provisions target controversy, involve the opt-in versus opt-out concepts, and the affiliate protection provisions.

Robert J. Warner, the New York State Assemblyman, has said that probably no New York State legislation is going to happen this year. That may or may not be true in the other legislatures around the country. In the enforcement area, we have had two active state Attorneys General, Michael Hatch in Minnesota and Eliot Spitzer in New York, who have, I believe, worked out individual settlements with the institutions involved. One commentator describes these settlements as being more onerous to the institutions than the provisions of Gramm-Leach-
Our first panelist is Oliver Ireland, Associate General Counsel of the Federal Reserve System. He has been with the Board for fifteen years. Before that, he was at the Federal Reserve Banks of Boston and Chicago.

MR. IRELAND: I am just going to give a very general overview — as long as time allows.

The issue of privacy of financial information is a difficult one. On the one hand, it is very clear that individuals place great value on the confidentiality of their personal data, and they place particular importance on the confidentiality of their private financial data. For example, there are common law cases dating back to the 1920s finding implied contract provisions, between banks and their customers, and requiring the banks to hold customer data confidential.

At the same time, broad dissemination of data about people's financial choices is economically efficient. Our Chairman is particularly fond of an example that goes something like this. If producers of coats know that people will only buy red coats, they won't produce any blue coats. If they don't know that and produce

---

15. See id. ("Citigroup Privacy Promise, the firm's current privacy policy statement, provides several protections beyond those of [Gramm-Leach-Bliley], including an opt-out for certain affiliate sharing.").
17. See Alan B. Vickery, Note, Breach of Confidence: An Emerging Tort, 82 Colum. L. Rev. 1426, 1430 & n.14 (1982) [hereinafter Vickery] (discussing how the English case Tournier v. National Provincial & Union Bank, 1 K.B. 461 (C.A.) (1924), determined that confidentiality was implied in a deposit contract and how that case was relied upon by American courts); see also Peterson v. Idaho First National Bank, 83 Idaho 578, 588, 367 P.2d 284, 290 (1961) ("[I]t is implicit in the contract of the bank with its customer or depositor that no information may be disclosed by the bank or its employees concerning the customer's or depositor's account, and that, unless authorized by law or by the customer or depositor, the bank must be held liable for breach of the implied contract."); Susan M. Gilles, Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy, 43 BUFFALO L. REV. 1, n.86 (1995) (naming other American cases that have found that the implied contract between a customer and a bank includes confidentiality).
the blue coats, the cost of producing blue coats is waste, whereas the cost goes up for red coats. Disseminating information about those choices drives the cost of goods and services down and increases standards of living.

So you have this difficult problem of balancing the personal interest of privacy — that I think we all recognize and that certainly is recognized in our Constitution\(^9\) — against economic efficiency. This, added to the traditional consumer conflicts that are typical in the consumer financial services area,\(^2^3\) represents the balance between the interests of individual institutions and the interests of customers. This balancing must be sorted out by the time we get to legislation, causing a very complex matrix of interests that is present in almost all statutes.

This issue came up in Gramm-Leach-Bliley, I think, perhaps just by accident. There had been a number of events in Washington, at least in the last few years, which indicated a lack of understanding by individual consumers about how their data was used by the various people with whom they did business. The biggest problems in Washington were CVS Corp. (CVS drug stores) and Giant Food Inc. (Giant Supermarkets).\(^2^1\) Both had pharmacies that used a data processor to process prescription information. The data processor also did some marketing on the basis of the information that it processed. This story was publicized in the *Washington Post*.\(^2^2\) CVS, I think, was the holdout. It kept its contract with that data processor for maybe a week or

\(^9\) See e.g., *Griswold v. Connecticut*, 381 U.S. 479 (recognizing the existence of a constitutional right of privacy).


\(^2^2\) Id; see also O'Harrow, *CVS also Cuts Ties to Marketing Service; Like Giant, Firm Cites Privacy on Prescriptions*, WASH. POST., Feb. 19, 1993 (Financial), at E1.
ten days. Giant gave it up virtually immediately because the outcry was so vociferous.24

I think recognition that there were privacy problems in the financial area, somewhat illuminated by Minnesota Attorney General Hatch25 and his actions, raised similar concerns in Washington.26 At that time there was an interesting vehicle going through Congress — Gramm-Leach-Bliley. Gramm-Leach-Bliley's intent was to allow banks, which some people thought of as isolated institutions and which have been historically separated from other financial institutions by statutory provisions, broader cross-industry affiliations. This gave privacy advocates an opportunity to argue that broader affiliation would result in a broader dissemination of data.27 The result was legislative provisions dealing with the privacy issue.

Privacy advocates' appeals resonated with people on both sides of the aisle. This was not necessarily a partisan issue. We had both Democrats and Republicans strongly in favor of privacy requirements.28 What resulted was a notice and opt-out system for people's personal financial information at financial institutions. Financial institutions include banks, broker-dealers, insurance companies, and a whole host of other institutions yet to be defined by the Federal Trade Commission ("FTC").29 Basically, the system

23. See Robert O'Harrow, supra note 22 (discussing CVS's defense of its contract with Elensys Inc., "a computer database specialist that also mails out drug information on behalf of pharmacies").
24. See id. (noting that CVS gave up its contract with Elensys only after Giant made an announcement that it was cutting ties to Elensys).
25. See OAG homepage, supra note 14 and accompanying text; see also sources cited infra notes 89-90.
27. See generally 145 Cong. Rec. S13883 (1999) (containing statements by senators, including Senators Feinstein, Boxer, and Harkin, opposing the Gramm-Leach-Bliley Act because it does not prevent the disclosure of information, such as credit card balances, bank statements, and mortgages).
covers any entity that engages in business activities that financial services holding companies traditionally have engaged in.

Gramm-Leach-Bliley says that those financial institutions have to give their customers a notice describing their privacy practices, specifically before they share any of their customers' data with a third party for marketing purposes.\(^3\) I think disclosure to the newspapers would be subject to the same notice requirement. Generally, before financial institutions share customer data for marketing purposes, they have to give consumers a way to opt-out of that disclosure, and then honor any opt-out that follows.\(^3\)

Obviously, because a lot of this is related to financial transactions, there is a long list of exceptions to be found in the statute.\(^3\) One exception allows banks to conduct processing in the ordinary conduct of business, as it has historically been known, without being subject to the opt-out requirement.\(^3\) What it boils down to is that the opt-out is principally a marketing issue. Congress went on to do something that was more or less unprecedented. Congress required that the financial supervisory agencies\(^3\) write and implement standards to safeguard personal information for their respective jurisdictions.\(^5\) Further, it urged them to write joint rules so that the rules would be identical.\(^5\)

Normally in the consumer protection area, one agency is

---

31. Id. at 15 U.S.C. § 6802(b) (outlining opt-out procedures for disclosing personal information).
34. These agencies are the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Company, the Office of Thrift Supervision, the National Credit Union Administration, the Federal Trade Commission, and the Secretary of the Treasury, in consultation with the insurance authorities of the States.
36. Id. at 15 U.S.C. § 6804(a)(2) (requiring that agencies work together to ensure “coordination, consistency, and comparability” of their respective regulations).
designated as a rule writer — if you are going to have a rule writer — on grounds of efficiency. In the spirit of democracy, though, they made this a joint rule-writing effort. Then, to top it off, they made it an accelerated rule-writing effort. They required the agencies to have final rules in effect six months after the effective date of the statute. Those rules go into effect for financial institutions one year after the effective date of the statute, unless later deferred by the agencies.9

We have been in the process of an inter-agency rule-writing effort. We put out rules, depending on which agency you talk to, either early or late in February, that are more or less identical. There are some very minor differences between them. At this point, we have an unknown number of comments. I have seen probably 2,000 myself, including a write-in campaign from the National Association of Private Investigators and a write-in campaign from consumers based on a newspaper article in Denver, in addition to every major financial institution, trade association, and major financial institution commenting.

We are in the process of trying to sort this out. We have some speakers here today from major New York banks who I think can

37. Id.
42. C.f. id.
43. Pamela Yip, Financial "Buffets" on the Way, THE DENVER POST, Feb. 27, 2000, at M-09 (balancing the consolidation of consumer financial needs with the protection of consumer personal information).
44. Jay Soloway, Senior Vice President and Associate General Counsel to Chase Manhattan Bank and Carl Howard, Vice President and Associate General
tell you in greater detail about the specifics of the rules and the specific problems they raise and the issues surrounding those.

MR. MITCHELL: Thank you, Mr. Ireland.

Our next speaker is Jay Soloway, who is Senior Vice President and Associate General Counsel to Chase Manhattan Bank. Mr. Soloway?

MR. SOLOWAY: Thank you, Mr. Mitchell. Thank you to Fordham University for inviting me to participate in this forum.

Interestingly, when I am asked to talk on this subject — and it has been a subject on a lot of people’s minds over the last several months, if not years — one of the things I usually like to do is poll the audience to find out what they think they mean by “privacy.” I am not going to do that now because of time, but let me give you some of the themes that usually come up when I do this. People usually say, “Oh, I think it’s the right to be left alone.” That is a standard some of us have heard before. Some say, “It’s keeping my information secure and protected.” Some talk in terms of freedom from fraud and abuse, such as things like identity theft. Others say, “It’s the ability to contain and to have my information not disclosed.” That is just a handful of the responses I receive.

What is interesting is that everybody has a different definition of privacy. Not only do they have a different definition, but often they have very different perspectives, which may become evident in the discussions of this panel.

There is a very technical perspective. Lawyers like to focus on the technical perspective of things and analyze the words, content, meaning and so forth. There is a very emotional perspective that this engenders with people because it has to do with their information and how it is used — or, in their minds, maybe misused. There is most certainly a political aspect to it, which I think Mr. Ireland alluded to in his comments.45

What it comes down to, it seems to me, is that consumers have a legitimate interest in privacy of their data. I would also argue that financial service providers have an equally legitimate need to gather and use information about their customers and consumers. Sometimes it is for their benefit, for the benefit of the consumer for

45. See discussion supra pp. 72-73.
fraud prevention, or for the benefit of the institution. Sometimes, it is to expand consumers’ options and choices in services offered to them. Sometimes it is to enhance the service quality that they receive from institutions. All in all, what you start with is a very broad category of privacy and data sharing, and it is hard to know where to begin approaching the subject in any given instance. Congress, in its wisdom, chose to use the vehicle of the Gramm-Leach-Bliley Act to take one of its first federal forays into this issue. Prior to Gramm-Leach-Bliley, there was a lot of discussion on medical information, which is also a very sensitive area, but I don’t think it was politically ripe at that time for Congress to use medical information as a vehicle.

I heard only a little this morning — and I apologize for not being here for the whole session — so I may repeat a few things. We hear a lot of people talking about the Gramm-Leach-Bliley Act. What I like to remind people is that it is also called the Financial Services Modernization Act, not just the Gramm-Leach-Bliley Act, and the intent was to modernize the financial institution arena. There was a great recognition by Congress that the economy, the industry, and the marketplace were moving. I think

46. See Arber Veverka, *Balancing Privacy and Commerce; Rules Detailing How to Carry Out New Federal Law are in the Works*, CHICAGO TRIB., Feb. 8, 2000 at C3 (“[t]he Gramm-Leach-Bliley Act’s protection is the first overarching federal privacy law ever crafted”).


48. A bill entitled The Medical Financial Privacy Protection Act, H.R. 4585, has been proposed in the House of Representatives to amend Gramm-Leach-Bliley by prohibiting financial institutions from sharing their customers' personal medical information with affiliates and third parties. See http://www.namic.org/lss/hr4585.htm (last visited Oct. 3, 2000).


they will now admit it had already moved by the time the Financial Services Modernization Act came into place.

The privacy issue did come up late in the agenda. Most congressmen recognize the fact that we are financial information providers and that we are an information industry. They would also recognize that we are becoming an information culture. Consequently, what Congress did was support the pro aspects of cross-marketing and the pro aspects of combining industries. Inherent in financial modernization is the movement of data within the covered organizations.

We have heard that banks might combine with securities companies and, in turn, might combine with insurance companies. In fact, if you look back, you will see that even banks themselves were made up of multiple institutions way before this Act came about. My own organization, Chase Manhattan, in its more traditional role as a banking institution, had 500-plus companies associated in it.

There is a need to deal with consumers in a holistic way. There is a need to use that information on behalf of the consumer across those multiple entities. A bank used to be a single organization. Nowadays, or even before the Financial Services Modernization Act, it might have also consisted of a depository institution, or several; it might have also consisted of a credit card company; it might also have consisted of a mortgage company.

51. See 145 Cong. Rec. § 4918 (1999); see also supra text accompanying note 2.


55. See e.g., Capital City Group Announces $.12 Per Share Dividend, PR NEWSWIRE, Aug. 26, 1999 (noting that Capital City offers traditional deposit and credit services, asset management, mortgage banking, credit cards, data
Reasons for this are beyond this discussion. Suffice it to say there were legal, geographical, and regulatory issues that necessitated the need to have multiple companies.

Consequently, when you hear the subject that comes up from time to time of affiliate sharing, people automatically think that it is a bad thing. In reality, our affiliates exist for many different historical reasons. It’s the same information used by one family of companies to benefit that same consumer, regardless if it is in one organization or multiple organizations.56

The Financial Services Modernization Act also addressed a subject that I am not going to touch much upon, but if you just look in today’s New York Times,57 you will see it is a topic still of great interest — identity theft. In the privacy protection section of the Act,58 sub-part b enhances the criminal aspects of fraudulently obtaining customer information from a financial institution.59 The information is then used to steal a person’s identity and commit further fraud by obtaining credit, deposits, loans, or rental properties, etc. That subject is addressed in Title V of the Act.60

What I have heard several people say, and may hear others say in the future, is that the Financial Services Modernization Act didn’t do much for the privacy arena.61 In fact, I think it did a lot for the privacy arena. It took whole new provisions that financial institutions are going to have to apply, some of which Mr. Ireland

56. See generally Prepared Testimony of Professor Fred H. Cate on Behalf of the Financial Services Coordinating Counsel, FED. NEWS SERVICE, Apr. 12, 2000 [hereinafter Cate] (“many benefits... have resulted from responsible information use”).


59. See id. at 15 U.S.C. § 6821 (a) and (b).


61. See e.g., Testimony Commerce Trade and Consumer Protection, FED. DOC. CLEARING HOUSE CONG. TESTIMONY, Apr. 3. 2001 (“The much ballyhooed privacy provision of the Gramm-Leach-Bliley Act does not protect consumers’ privacy.”).
mentioned before, to bring information, disclosures, and options to their customers. It is not that we were not doing this in the past. Financial institutions have always cherished the information they have about their customers. They cherished it because it was a matter of trust, and there is nothing that a financial institution would do to violate that trust intentionally.

The difference is that we now have methods imposed by regulations to deal with this problem. That is different from the private sector coming up with their own ways of showing individuals how they deal with information in a trusted manner. There are a host of things that have to be done now, since the adoption of the Financial Services Modernization Act. What do we have to do? We are going to have to analyze the final regulations when they come out. We are going to have to adopt new policies and procedures — not necessarily to change what we were doing, but just to restructure them to comply with the way the Act says we have to disclose it. We will have to create disclosures, paperwork, and give them out to people individually and then mail them out annually. This is a significant cost factor considering

62. See supra text accompanying notes 29-31.
63. See e.g., "First Data Direct Banking Extends Industry - Leading Security Certification to NetPrecision Client Web Sites, BUS. WEEK, Apr. 15, 1999 (encouraging the use of ICSA TruSecure web certification and its Privacy Policy Program by client financial institutions to further internet banking); VASCO Data Securities Reports Year-end Results, 1993 Revenue and Operating Income Increase Over Prior Year, PR NEWSWIRE, Feb. 16, 1999 ("providing information security solutions that help organizations increase revenue and market share, build customer loyalty, expand online services, and protect critical information assets").
65. See Cate, supra note 56 ("implementation and compliance with these provisions are going to be complicated and time-consuming, ... sending as many as two and a half billion notices to their various customers by December 12 [2001]").
there are thirty-five to forty million customers around the country. In addition, we must have practices and procedures in place to deal with the regulations.\textsuperscript{66} We must have technology in place to capture back the requests and preferences of individuals in a multi-company, a multi-product, or a multi-geographic arena.\textsuperscript{67}

When you tell an institution that you don’t want your information shared with a third party, maybe that’s applicable for the marketing of pots and pans and magazines. Maybe it’s not applicable when you want to receive information about other financial products or services that we ourselves don’t offer directly but we might want to partner with another type of entity to offer. It could be a product opt-out;\textsuperscript{68} it could be a geographic opt-out; it could be an entity opt-out. Maybe you are concerned about your mortgage information, but you are not so concerned about your deposits, or vice-versa. It is up to you, but we have to have the mechanism in place to track and do this. For instance, if there are joint account holders, does one account holder have the right to speak for both, or should we track individual joint accounts?\textsuperscript{69}

These are just a few of the things that we are going to have to deal with in this regulation, and it is going to be extremely costly to

\begin{itemize}
\item \textsuperscript{66} See Cate, \textit{supra} note 56 (requiring “implementing, complying with, and overseeing these new regulations”).
\item \textsuperscript{67} See Cate, \textit{supra} note 56 (“The costs of establishing privacy policies, training employees, setting up internal mechanisms to coordinate differing information systems between subsidiaries and segregating the information of those that opt-out will also be high. So will [the cost of] establishing new security systems and systems for monitoring overall compliance with the Act.”).
\item \textsuperscript{68} See e.g., Privacy Rights Become Focus for Proposals in Congress, \textit{AM. BANKER}, Jan. 25, 1999 at 1 (a staff member for Representative John L. LaFalce suggested that “a customer could opt out by product line, perhaps allowing disclosure of account information but rejecting sharing of loan application data”).
\item \textsuperscript{69} For example, Washington Mutual’s opt-out policy applies to all members of a joint account. See http://www.wamuloanservice.com/xvrui/privacy.asp (last visited Oct. 15, 2000). Huntington Bancshares Incorporated (Ohio) has an opt-out policy that only opts-out on behalf of the requesting member of a joint account. See http://www.huntington.com/footer/HNB3800.htm (last visited Oct. 15, 2000). Ameritrade’s opt-out policy allows both options, allowing an opt-out request to apply to all members of a joint account or just the member requesting the opt-out. See http://www.ameritrade.com/tell_me_more/privacy_question10.fhtml (last visited Oct. 15, 2000).
\end{itemize}
do so. One questions whether Congress knows the best way to deliver this to individuals or whether individual institutions as a free marketplace should be able to develop it, and in fact distinguish themselves between institution A or B to offer the customers. If it's a valued right that a customer has, they should be able to see the differences between those institutions and not homogenize it under one scale.

I do want to point out that financial modernization and privacy are not new to us from the regulatory and legal perspective. Mr. Ireland alluded to court cases that have dealt with the issue. There is a whole long list of federal regulations that have existed over time, with at least some element of data sharing and customer information associated with them: the Truth in Lending Act ("TILA"); the Truth in Savings Act; the Fair Credit Reporting Act, one of the more significant provisions; the Electronic Fund Transfer Act ("EFTA"); the Telemarketing and Consumer Fraud and Abuse Prevention Act ("TCFAP"); and, last but certainly not least, the various state unfair and deceptive trade provisions with which we all have to comply.

Some have said that, as I indicated, the financial modernization and privacy legislation is not enough and that there ought to be new or further enhanced provisions put in place either at the federal level or at the state level. I think Mr. Mitchell touched upon one of the perspectives that my institution, and I

---

70. See supra text accompanying notes 17-20.
77. See Nahra, supra note 6.
78. See Star, supra note 5.
suspect most financial institutions, share. We have an Act that is just taking place, we have regulations that are just being enacted as we speak and that will be enacted sometime later this year, or maybe even a little later if the regulators recognize the enormous task that has to take place to put this into effect. All this suggests that what we have is insufficient or is not dealing with the privacy issues — which are yet undefined — in a broad enough manner. This may be extremely premature.

The other fear is that the states, while not invited, are given the authority to adopt legislation that is inconsistent with the federal provision as long as that inconsistency is more onerous or creates a higher standard.\(^9\) I think it would be inopportune for states to jump in without providing the opportunity for this legislation and regulation to, at least, play out a little bit and see whether there are any issues that need to be assessed and taken care of.

For an institution like my own, and many others, that tries to do business on a national scope, it would be nearly impossible — or extremely burdensome — to try to deal with multiple state laws and regulations requiring disclosure.\(^8\) Each state may apply a slightly different rate or apply it for a different product in each state. It would stifle an institution trying to offer programs on a national basis.

In addition, let me point out, for those of you who haven't read the Act, that the federal government also recognized the possibility that there might be a need for additional legislation. In fact, they call for a study in the Act.\(^8\) The study should be done to determine whether or not information sharing with third parties and affiliates needs to be the subject of additional legislation.\(^8\) I think the report is to be produced by January 1, 2002.\(^8\)

So there is already a recognition that “let this work, let us see what else needs to be done, and let’s give it some time.” Again, it


would be premature for others to act at this time. Let me point out in the last couple of minutes specific provisions in the proposed regulations that I am hoping will be further addressed as the federal regulators look at the comment letters. First, what is the definition of a financial institution? The banking agencies, I think, would take a fairly broad look at what a financial institution is; looking at the Federal Banking Act\(^4\) itself to determine the authorities or powers of a financial institution.

The Federal Trade Commission on the other hand, was a little concerned about the breadth of that definition and suggested a standard that had the phrase “significantly engaged in financial activities”\(^5\) as part of the definition. What troubles me about this narrower approach, the FTC approach, is that there can be a large institution — for example, an Internet Service Provider or an Internet offering of some kind — that is gathering consumer financial information and using it, without being subject to the requirements of the Act and the regulations simply because it is not significantly engaged in financial services. If it is a $1 billion business and only five percent of its operations are financial, then maybe it would not be considered a financial institution.

I would argue, instead, that any institution that gathers consumer financial information, particularly non-public personal financial information, as the Act and the regulations would define that, should protect that information the same way. A consumer and a customer should have the right and expectation to have that information treated the same way, regardless of whether it was acquired by the more traditional financial institution, or, as we go into the new century, by the non-traditional financial service provider.

Second, a core element that I think still needs to be addressed is what is non-public personal financial information?\(^6\) This is a

\(^{84}\) 12 U.S.C §24 (2000).

\(^{85}\) 16 CFR § 313.3(l)(1)(Federal Trade Commission definitions).

\(^{86}\) Section 509(4) of the Gramm-Leach-Bliley Financial Services Modernization Act defines it as “personally identifiable financial information” given by a customer to a financial institution. The Securities and Exchange Commission altered the definition to exclude information obtained by a broker-dealer, fund, or registered advisor, reasonably believed to be lawfully available to the general public from (1) the financial institution, if the customer states that the
subject that Mr. Ireland and I have discussed from time to time. The regulations as they come out have several pages devoted to this subject. Yet I am hard pressed to find a reason why they find any information that a financial institution has about a consumer is non-public personal financial information.

It is the "any information" that troubles me, because I think it disregards the whole concept of what is confidential information and what is financial information, or what is public versus non-public. There is some language in there trying to distinguish public and non-public, but I do not think it goes quite far enough.

I would ask people generally, whether they think their name, address, and phone number is non-public financial information. I would think it is not, since in the majority of cases you can find that information in any phonebook or on many Internet sites or by many other easily accessible means. One, I do not think it is non-public information; I think it is public. And two, I do not think it is financial information. In fact, there was a colloquy in the enactment of the statute that concluded that financial information had to do with the financial content of the information that you had.88 Gramm-Leach-Bliley is really geared towards items such as your balances, your credits outstanding, and so forth. It is not simply, whether you have an account with a bank, a securities company, or an insurance company?

I am not sure people would think that is non-public, nor do I think it is financial. Most of us issue checks every day and most of us have our names and addresses on those checks. Very many of us also use credit cards to charge, and that simply says you are a credit card customer of that institution. In fact, there are a whole lot of people these days who will sign up for one of a thousand Internet services and give out a wealth of information about themselves, not knowing anything about to whom they are giving such information. Perhaps, the definition that apparently is

---

88. Cf. source cited supra note 34.
espoused in the regulation is trying to restrict more than what was intended by protecting the true non-public personal financial information.

MR. MITCHELL: Thank you. I wonder if I could ask you a question. I do not want you to divulge any of Chase's strategy, but I believe that you entered into some sort of an agreement with New York State in January, and I think U.S. Bancorp entered into a similar agreement with Minnesota. They are the two that I am aware of, although there may be others. Do you see these types of arrangements as increasing? Do you see other financial institutions doing the same to avoid hassle, and really going further than Gramm-Leach-Bliley requires one to go?

MR. SOLOWAY: I will give you two comments on that. One is that yes, we did enter into an understanding with the New York State Attorney General. I think a lot has been said about that as going beyond the requirements of the Financial Services Modernization Act. The truth of the matter is that we had already instituted the majority of the things that we announced as part of our agreement with the Attorney General by the time the Attorney General had even started to investigate the issue. I am not going to comment on whether they were investigating it because they thought it was a real problem in the industry or with Chase, or whether they felt it was a political opportunity to seize upon an issue that was very public at the time.

Heading towards the second part of your question, for financial institutions that have a strong dedication and

---

89. Chase Manhattan and the New York State Attorney General's Office agreed that the bank would no longer share private financial information about its customers with unaffiliated third parties, including telemarketers. See Kathleen Day, Chase Settles Privacy Complaint; Bank, New York Reach Agreement, WASH. POST, Jan. 28, 2000 at E4; see also supra note 14 and accompanying text.


91. Id.
commitment to privacy and have an image to uphold in a community, it does not serve them well to do battle with government representatives on issues like this in the public forum. Even if you believe you are right and you have done nothing wrong, there is a great deal of pressure that comes to bear when it appears — even if it is not true, but it appears, I emphasize — that you are trying to oppose privacy standards for your customers and your customers are not following practices that others think are warranted. So the pressure that comes to bear in some cases may be due to actions that you have taken; but, in certain cases, it is simply due to a matter of perception in the marketplace.

There is a task force\(^2\) that exists now of at least twenty Attorneys General that have been working on this issue and that have already contacted many financial institutions around the country. I think that many of them are putting that same pressure on other financial institutions, that I think will be placed in the same position and confronted with the same decisions that Chase was, whether the wish to stand up their beliefs, that what they have done is right and so forth, or maybe take a simpler course of action, agreeing to do things that in fact they had already been doing.

MR. MITCHELL: Thank you, Mr. Soloway.

Our next speaker is Carl Howard. He is General Counsel for Bank Regulation at Citigroup.

MR. HOWARD: Good afternoon.

I am going to talk briefly about the constitutional implications of privacy restrictions. I'll talk about opt-ins versus opt-outs as a privacy remedy. Finally, I am going to talk a little bit about privacy polls.

When a legislature enacts privacy restrictions, it may not think

---

\(^2\) See Orla O'Sullivan, Making Internet Banking Safer for the Customer, U.S. Banker, available at http://www.us-banker.com/usb/articles/usbjan-2.html (last visited Aug. 11, 2000); see also Comments of Attorney General to Joint Agencies' Proposed Rules (OCC, OTS, FRB, FDIC), 651 Fed. Reg. 8769 (Feb. 22, 2000), available at http://www.naag.org/features/privacycomments1.cfm (last visited Oct. 11, 2000) ("It is essential that the final regulations expressly prohibit financial institutions from entering into marketing agreements that permit any non-affiliated third party to charge a customer's credit card or debit a customer's account without first requiring the consumer to explicitly agree to the purchase.").
about it this way, but it is usually enacting a restriction on speech, as that term is understood in the First Amendment context. We have a line of Supreme Court cases, starting with Virginia Board of Pharmacy93 in 1976, which holds that the First Amendment protects commercial speech.94 In fact, you will probably remember that a lot of these cases involved attorney advertising.95

The constitutional protection for commercial speech is a qualified protection. It is not the relatively absolute protection that exists for political speech.95 You have the situation when that somewhat protected constitutional right comes into conflict with another constitutional right — the right to privacy — there can be an interesting conflict.

A recent case that rules on this conflict in a relevant context to the kind of discussion we are having today is the decision of the Tenth Circuit in a case called US West.97 US West involved an FCC regulation that required telephone companies to secure customer consent before they use customer-calling data to solicit telephone services from their existing customers.98 The Tenth Circuit found that the FCC regulation was an unconstitutional restriction on US West's right of commercial speech.99

We have a consensus that the controlling case here, and the case that the US West court relied on, is a 1980 Supreme Court

---

94. Id. at 780-81 (distinguishing between commercial speech and ideological expression and holding that commercial speech was protected because it was "information of potential interest and value").
95. See Bates v. State Bar of Ariz., 433 U.S. 350 (1977) (holding in part that "advertising by attorneys could not be subjected to blanket suppression"); see also Ohrilik v. Ohio State Bar Ass'n, 436 U.S. 447 (1978) (holding that attorney's aggressively solicitation of accident victims was not protected by the constitution "because the state had a legitimate interest in preventing aspects of solicitation involving undue influence and other forms of vexatious conduct").
97. U.S. West, Inc. v. F.C.C., 182 F.3d 1224 (10th Cir. 1999).
98. Id. at 1228.
99. See id.
decision called *Central Hudson.*\(^{100}\) *Central Hudson* gives a four-part test to decide what to do with a restriction on commercial speech. The Court said in *Central Hudson* that (1) first, speech must be lawful and not misleading; it can definitely be blocked by the legislature if it runs afoul of that.\(^{101}\) But, if we assume that it is both lawful and not misleading, the Supreme Court said that (2) you ought to ask whether the legislature has a substantial interest in regulation of the speech in question;\(^ {102}\) (3) whether the regulation directly and materially advances that interest;\(^ {103}\) and (4) finally, whether the regulation is narrowly tailored to fit the desired objective.\(^ {104}\) If we assume lawful and non-misleading speech, as I suggested before, privacy will usually qualify as a substantial state interest — or federal interest, for that matter.

But the third and fourth parts of the test\(^ {105}\) from *Central Hudson* are highly judgmental. The *US West* court, the Tenth Circuit, thought that the FCC’s privacy concerns were arguably legitimate, but it reversed in *US West* because it found that the opt-in that the FCC required US West to use was overkill.\(^ {106}\) Instead, the *US West* court said that an opt-out would have worked just as well, without having the constitutional infirmity vis-à-vis free speech.\(^ {107}\)

If you look beyond the *US West* case, you will find that there are Supreme Court and Court of Appeals cases that address this conflict between privacy rights and commercial speech rights, and that they are essentially all over the place.\(^ {108}\) You can find a

101. *Id.* at 563, 566.
102. *Id.* at 564, 566.
103. *Id.*
104. *Id.* at 565, 566.
105. *See id.* at 564-566.
107. *Id.*
holding that stands for just about any proposition you want in this area. But I think the one thing that you can say with some certainty is that when a legislature thinks about this kind of issue, the broader and more pervasive the restriction they enact, the more likely it is to have a constitutional problem that will result in a negative balance of the kind the US West court found. So the lesson I would get out of this is that legislators ought to be thinking about doing a balancing exercise and not thinking of privacy as simply an absolute right that trumps all other rights.

Now let’s talk about the kinds of choices that legislators have when they fashion privacy remedies. There is a continuum of available privacy remedies. If you start over on one side, hypothetically — sorry, Mr. Soloway — you have done nothing. Moving up from there, you have something that you might label

New York City Parks Department Use Guidelines specifying that the City would furnish and operate sound equipment used in Central Park concerts constitutional under the First Amendment because the guideline met governmental interests without regulating content); Members of the City Council of the City of Los Angeles v. Taxpayers for Vincent, 466 U.S. 789, 104 S. Ct. 2118 (1984) (deciding that a local ordinance prohibiting the placement of signs on public property did not violate the First Amendment because the ordinance was not content specific and served a “sufficiently substantial” esthetic governmental interest in maintaining the quality of life of its citizens and maintaining property values); United States Postal Serv. v. Council of Greenburgh Civil Assoc., 453 U.S. 114, 101 S. Ct. 2676 (1981) (holding that a statute prohibiting a non-profit group from placing unstamped mail into the mailboxes of private homes was constitutional because mailboxes are not within the public domain); Bailey v. Morales, 190 F.3d 320 (5th Cir. 1999) (holding that a state law prohibiting the solicitation of chiropractic patients based on a pre-existing condition was unconstitutional because the statute did more than protect proper state interests); Falanga v. State Bar of Georgia, 150 F.3d. 1333 (11th Cir. 1998) (deciding that a Georgia law prohibiting lawyers from soliciting clients face-to-face was constitutional under the First Amendment); Pearson v. Edgar, 153 F.3d 397 (7th Cir. 1998) (finding that an Illinois statute that aimed to prevent real estate agents from persuading owners to put their homes on the market because of fear that the racial composition of the area was changing violated the First Amendment because the state failed to justify how the statute advanced state interests); Van Bergen v. Minnesota, 59 F.3d 1541 (8th Cir. 1995) (finding that a statute regulating automatic dialing-announcing devices was constitutional and did not violate the First Amendment because the government was protecting the privacy of its citizens without considering the contents of the speech).

109. Id.
“full disclosure,” telling your customers what you do. Coming up further, you have an opt-out remedy. Further still, you have an opt-in remedy; and then, finally, you have absolute prohibition.

Every step up the continuum involves an increase in the cost and regulatory burden and a reduction of free market functioning as a way to allocate resources. Every step up the continuum is a decision that the government ought to be intervening and reducing free market functioning as a way to allocate resources and to make decisions. Now, as to the first step on the continuum, doing nothing may not sound like much of a privacy remedy, but it makes a lot of sense in a free market economy, if the problems that you are thinking about appear more hypothetical than real. In a free market, the presumption should always be against regulation because regulation always distorts free markets and always has costs associated with it. Therefore, the party that asserts the need for regulation should have the burden of demonstrating that need fairly convincingly.

In Title 5 of the Financial Services Modernization Act, Congress rejected a do-nothing option, as we have been discussing, and opted instead, for affiliate sharing — sharing of information within a financial services conglomerate. Congress decided that a full-disclosure option was the way to go. So it went one step up on the continuum of privacy remedies.

Disclosure is, of course, a remedy that is widely used in our country to ensure that consumers have adequate knowledge on which to base their decisions. Potential consumers who do not like the affiliate-sharing arrangements that are laid out in the privacy notice that financial institutions are now required to give can decide that they do not want to do business with that company. In a market with many financial services providers, some of whom will be competing on the basis of the privacy protections they are affording to their customers, these are meaningful choices. There

110. See, e.g., Peter Vandoren, Strangulation by Regulation: How It Happened; What To Do, NAT'L REV. Vol. LII, No. 8 (stating that forty years of scholarly research shows that markets have been regulated unnecessarily and that “[r]egulation usually benefits a privileged group, makes everyone worse off than they would have been regulation, or does both”).

are tons of banks, securities brokers, and insurance underwriters out there to choose from. They will have different privacy policies and they will be telling people what those policies are and letting them choose their financial services providers on the basis of those policies.

As to third-party information sharing, as we have heard, Congress went a step further on our continuum of remedies and it mandated a user-friendly opt-out procedure. A formal opt-out provision gives a consumer an important right of choice that goes beyond the sort of market opt-out that exists when a consumer chooses one service provider over another, because it lets the consumer say, "I want to do business with you and I don't want you to share the information with third parties."

Think about the question, "Okay, if that is good, what is wrong with an opt-in as opposed to an opt-out?" You might say to yourself that an opt-out versus an opt-in is simply two different ways to set the default option. Alternatively, you can think of them as burden-shifting devices; they decide who has the burden of going forward. It is important to recognize that an opt-out provision gives essentially the same consumer protections as an opt-in, but without the significant procedural burdens and compliance costs that are associated with opt-ins.

Opt-ins are essentially impossible to use with existing customers because, no matter how many times you mail a form to your customer and no matter how many times you call them on the phone to talk to them about this, they generally will not respond. This does not necessarily mean that they are responding negatively; they are simply not responding. Even for new customers, an opt-in makes a default choice for the customer that is hard to rationalize, given where we are today.

Opt-ins are difficult to rationalize for affiliate sharing because they function as an anti-affiliation and an anti-cross-marketing

---

112. See Gramm-Leach-Bliley Financial Services Modernization Act § 502(b).
provision. In other words, an opt-in creates a presumption that cross-marketing is not a good thing. We have just decided in the Financial Services Modernization Act that our national policy is to favor financial services affiliation and to favor cross-marketing, and a default provision that is based on the opposite assumption does not make a lot of sense.

But I would suggest that even using such a default for third parties does not make a lot of sense in an economy that is very much an information economy. The information economy that we are in today is characterized by the free flow of information, and other industries participate fully in this free flow of information. Other industries not only do not have opt-in provisions, but they don’t have opt-out provisions. They don’t even have disclosure; they just share information. We are not doing anything to restrict that sharing of information. You may think we should restrict, but that is a much broader question than what we ought to be doing with the financial services industry. If providers of financial services are subjected to significant constraints on free flows of information when others are not, they and their customers will become second-class citizens of the new information economy.

Finally, if you think that opt-ins are the way to go because everybody knows that consumers are very concerned about privacy, then we would like to take you on a visit to the Citigroup privacy poll archive. In our poll archive we have a poll for whatever proposition you would like to advance about privacy that proves you are right and that no other view can be correct.

For example, we have a poll that says ninety percent of U.S. citizens are very concerned about privacy. We also have a poll that says seventy percent think that information gathering and sharing by commercial companies is a bad thing. We have another poll with a similar cross-section of U.S. adults. It starts by telling the respondents that commercial companies like to share information so that they can better understand what products each customer wants. This saves their customers from providing the same data repeatedly and allows the companies to offer discounts to customers who take multiple products, and so they can prevent fraud. And guess what? When you tell that to U.S. adults, seventy percent of them say, “Well, if that’s why you want to do it, then I think information sharing among commercial companies would be
a good thing.” We have a poll that says ninety percent of Internet users think that consumer information gathering at web sites is a good thing if it is fully disclosed and explained.

Finally, we have the poll that we think is actually the most meaningful poll. It is based on asking a lot of people a whole lot of questions about privacy. What it shows is that about twenty-four percent of the people in the United States are what you might call “privacy absolutists.” They generally do not want to share any information with anybody about anything. Similarly, sixteen percent of U.S. adults are “privacy unconcerned”; they don’t care who knows what about them and they are going on Oprah this afternoon to tell all. But the large majority, sixty percent, are “privacy pragmatists”: they say, “It depends. I may be a little bit concerned as to what the grocery store is doing with all that information they get when I swipe my Frequent Shopper’s card, but hey, if they are going to give me discounts in return for my data, I guess I don’t care.”

A complete prohibition on information sharing among financial services companies, or an opt-in which is the close cousin of a complete prohibition, makes sense if you think that seventy-five percent of the people in the United States are privacy absolutists. If, on the other hand, you think what this poll suggests, that absolutists are only twenty-five percent and about seventy-five percent are either privacy pragmatists or privacy unconcerned, then a blend of disclosure and opt-out is what makes sense. The good news is that is just what Congress did in Title 5 of the Financial Services Modernization Act.

Thank you for your attention.

MR. MITCHELL: Excellent. Thank you, Mr. Howard.

I wonder if I could ask you something. I guess my own reaction when somebody sends me something, a form letter from a financial institution, you’re right, I probably do not respond. I know that one of the big worries with the opt-in provision is that you are not going to hear back from anybody.

Do you have any other kind of client contact things you can base that on, where notices go out and you are supposed to get a return? Like proxies, do they ever get any proxies back?

MR. HOWARD: I think the US West litigation is useful on this point. US West first tried mailings to its customers to get them
to address this issue. They found that they could get only a five or ten percent response rate of any kind.  That is to say, ninety or ninety-five percent of their customers did not respond at all.

They then tried a telemarketing campaign, which, in theory, should have bumped the results up dramatically. It did get a higher response. About twenty-eight percent of the people said that they would opt-in; about thirty-three percent, or thereabouts, said that they would decline to opt-in; and forty percent of their customers said, "I don't want to talk about this," they declined to make a choice.  

So, is losing seventy-two percent of your customers better than losing ninety percent of your customers? Sure, if you think there is any merit to the kind of privacy poll data that I just talked about. A default choice makes sense. It is not a simple issue by any means.

MR. MITCHELL: Thank you.

Our last panelist, last but not least, Joel Reidenberg, is a Professor at Fordham. Joel?

PROFESSOR REIDENBERG: Thank you.

It was a pleasure to be able to suggest that I get to go last, since that means I get to be disagreeable with everything that was said before me.

MR. MITCHELL: They have the right of rebuttal. Everybody gets another round.

PROFESSOR REIDENBERG: Absolutely.

I wore my favorite conference tie for the purpose. For those of you who cannot see it, it's the Tin Tin character, which is a very famous French cartoon character that goes out battling the enemies and the bad guys. I think that is a good lead-in to what I have to say about the Financial Services Modernization Act.  

I would argue that the statute is in fact a weasel's response to privacy. If I were to give it a report card, I would give it a C-minus.

114. See U.S. West v. F.C.C., 182 F.3d 1224, 1239, n.12 (10th Cir. 1999) ("U.S. West also solicited approval [for use of private information] from customers by mail. Only six to eleven percent of residential customers and only five to nine percent of business customers responded to the direct mail trial type and bill.").

115. See id. at 1239.

As many of you know, I am a reasonably strict grader here at Fordham. A C-minus is pretty much the minimum passing grade you can get. If you get too many C-minuses, you flunk out of school. I really think that is what we see in the Financial Services Modernization Act. It certainly does some things that are valuable. I would probably agree with some of the observations that our co-panelists have made, and I will certainly disagree with others, and I am going to focus mostly on some of the things the statute does and what it does not do.

In looking at privacy, I think it is a mistake to view data privacy in the financial services context as merely associated with confidentiality in whether a bank or financial institution keeps data private from others, because that is only part of the problem, part of the issue.

There is a set of widely recognized data privacy principles that have been elaborated, first by the U.S. Government, codified by the OECD, subscribed to by the U.S. Government and every major bank here in New York. That set of principles sets out a whole series of standards for the treatment of personal information. It is really about allowing the citizen to participate in decisions about the collection and use of their personal information. That is really what this is all about.

I am going to use the term “citizen” willfully; I am not going to use the term “consumer,” because privacy is a citizenship issue.

117. Organization for Economic Cooperation and Development. The OECD is the successor organization to the Organization for European Economic Cooperation, which was formed as part of the Marshall Plan, to oversee American and Canadian aid to Europe after World War II. See http://www.oecd.org/about/origins/index.htm (last visited Dec. 11, 2000). Today, the OECD consists of thirty country members, who each make financial contributions to sustain the organization. See http://www.oecd.org/about/general/index.htm (last visited Dec. 11, 2000) (providing a forum to “discuss, develop, and perfect economic and social policy”).

118. The United States became a member of the OECD in 1951. See http://www.oecd.org/about/general/member-countries.htm (last visited Dec. 11, 2000).


120. Joel R. Reidenberg, Cyberspace And Privacy: A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules In Cyberspace, 52 STAN.
It is not just a business question. It is one that affects all of us. It is a political question. It has implications for political decisions.

When we look at the basic privacy standards, we see some very key elements:

Purpose limitations - if I am collecting information about individuals, it should be for defined purposes. If I use it for other purposes, I need consent. I need some form of permission. Whether it is opt-out or opt-in we can talk about, but the notion is there must be a purpose for which I am collecting the information. If I am not going to use it for that purpose, I've got to go back to the individual in some fashion.

Relevancy - is the data relevant to the transaction at hand? There is a presumption that it is not proper to go and engage in information grubbing, just asking for information because it is there, to amass profiles and warehouses of data about individuals.

Transparency - it ought to be transparent to the citizen who is collecting their personal information and how is it being used.

Accuracy - data should be accurate. Individuals ought to have an ability to access personal information about them and ask for correction of errors.

These principles must have some sort of enforcement remedies. Individuals ought to have a means to enforce their privacy rights. There ought to be sanctions if privacy principles are violated.

What do we see in the Financial Services Modernization Act? Not much. It focuses on disclosure. That's one element. That is


good. It's good that you have improved transparency. But it doesn't touch at all on purpose limitations.\textsuperscript{121} It doesn't touch at all on relevancy.

The enforcement remedies are "sort of." It establishes a very convoluted jurisdiction between different regulatory agencies and carves up enforcement to those regulatory agencies, but it creates no private cause of action. So the citizen whose privacy rights might be violated has no direct action under the statute. There are some indirect means we can talk about — whether it is a deceptive practice if this is disclosed — but the point is, as a privacy statute, this does not provide for enforcement remedies for the citizen directly.\textsuperscript{125}

It does make disclosure an important point. It focuses on transparency,\textsuperscript{126} at least providing one basic standard of privacy. Its scope of coverage seems to be broad where it refers to financial institutions, and then has what we've heard might end up being quite a broad definition of financial institutions. We'll have to see how that plays out. As a quick digression, I forget whether it was Mr. Soloway or Mr. Howard, — I think it was Mr. Soloway — who raised the point that there may be something anomalous if we regulate financial institutions but we don't touch other actors out there in the information economy trafficking in similar information. That is absolutely right. That is a major problem that

\textsuperscript{124} See Mierzwinski, \textit{supra} note 121 (Mr. Mierzwinski referred in his testimony to the notion that "information privacy law... promotes transparency." He also stated that "the Gramm-Leach-Bliley Act falls short of meeting Fair Information Practices in several areas... first, it fails to require any form of consent (either opt-in or opt-out) for most forms of information sharing for secondary purposes, including experience and transaction information shared between and among either affiliates or affiliated third parties... second, while consumers generally have access to and dispute rights over their account statements, they have no knowledge of, let alone rights to review or dispute, the development of detailed profiles on them by financial institutions.").

\textsuperscript{125} However, the Securities Act of 1933 and the Securities Exchange Act of 1934 did not create explicit private rights of action either, but the courts have allowed such actions nonetheless. See Steven A. Ramirez, \textit{Arbitration and Reform in Private Securities Litigation: Dealing with the Meritorious as Well as the Frivolous}, 40 WM AND MARY L. REV. 1055, 1067.

\textsuperscript{126} See Burk, \textit{supra} note 122.
we have in the United States. This statute does not touch that; it doesn’t really address that issue.

Let’s look at some of the things that the statute allows, such as sharing personal information with third parties, provided that there is an opt-out. The opt-out works on the basis of some disclosure — and we’ll find out, depending on how the final regulations come out, how meaningful the disclosure really will be. But it’s kind of interesting because one of the things that the Act does is prohibit sharing account identification numbers with third parties. I think this grew out of the U.S. Bancorp situation in Minnesota. But it does not say anything about sharing account balances with third parties, and it is not clear that the disclosure would make that so obvious to consumers. I think that is something that would certainly be a major concern for individuals doing business with their bank; if, for example, they were to discover that the bank is sharing their account balances with different third-party entities to offer them goods like grass seed for their house, or something like that.

The statute also allows for the sharing of information with affiliates. The statute essentially sanctions it and says it is perfectly legal. A citizen has no right to stop it and there is no legal right to stop that under the statute. The only restriction is that the bank has to tell you yearly that they are going to violate your privacy. They have to give you annual notice once a year that they are going to be sharing with affiliates.

Well, what does that mean? Let’s think about it. If it is a

127. See supra p. 85.
130. See supra OAG Homepage, note 14 and accompanying text; supra U.S. Bancorp Press Release, note 90 and accompanying text.
131. See Charles M. Horn, Financial Services Privacy At The Start Of The 21st Century: A Conceptual Perspective, 5 N.C. BANKING INST. 89, 99 (“[I]n the waning days of the fall of 1999, a series of last-minute compromises were reached among Senate and House leaders to modify the legislation’s privacy provisions to . . . permit financial firms to share customer information with affiliates . . .”).
132. See Gramm-Leach-Bliley Financial Services Modernization Act, Gramm-Leach-Bliley Financial Services Modernization Act §503.
bank, it might be the brokerage house; it might be an insurance company. Part of the importance of this statute for the financial services sector is we are expecting to see an increase in the nature and type of affiliations among financial institutions. This means that the range of entities with which information can be shared without the citizen having any right to say no is going to be expanding significantly.

Now, just think of all the different financial accounts you have. How aware are you of the identities of each of the different affiliates that your financial institution has? Chances are you probably have no clue, and the chances are if you asked the company, you'd have a hard time getting a clear answer.

The statute says that sharing of personal information with companies performing services for the financial institution is permitted without an opt-out.\(^{133}\) So if it's a company that is performing services for the financial institution or helping the financial institution offer a product, an opt-out is unavailable. If it is a joint marketing effort with another financial institution, as defined by what the Act and regulations will tell us, there is no need for an opt-out. They just need the initial notice.\(^{134}\)

There is a track record for unsolicited marketing of credit and insurance in the context of the Fair Credit Reporting Act.\(^{135}\) Such marketing is permitted under the Act, provided there is an opt-out. Companies will now go and say, “I’ll sell you a mattress on thirty days’ credit,” purporting that to be an extension of credit, therefore qualifying under the Fair Credit Reporting Act to gain access to your credit report.\(^{136}\) We can easily see that happening in this context.

If it is the Burpee Seed Company and they are going to offer grass seed to you on thirty days’ credit, is it now a financial product? If it is a financial product, the bank or any other financial institution can share the attendant consumer information. You

\(^{133}\) See Gramm-Leach-Bliley Financial Services Modernization Act § 502.

\(^{134}\) Id.

\(^{135}\) See generally Sandra B. Petersen, Note, Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?, 48 FED. COMM. L.J. 163 (1995) (discussing some of the shortcomings of the Fair Credit Reporting Act in the area of credit marketing and credit insurance).

have no right to stop it. So if you look at the way the regulations are structured, you can see a very strong incentive cropping up for some interesting structuring arrangements between sellers and financial institutions.

The statute makes a distinction between public and non-public information.\textsuperscript{137} We heard a little bit about that. This is particularly troubling from a data privacy point of view because the issue is what is being done with personal information, not where you get that personal information. It's how is a company treating personal information and what rights does a citizen have in participating in those decisions.

I think it is a real misnomer to categorize this battle as one of privacy against business. It seems to me that there is nothing harmful in saying that citizens ought to be entitled to participate in the decisions about them, particularly when the companies argue that the only reason for doing these cross-marketing and profiling activities is to benefit consumers. If the goal is to benefit consumers, then let them participate in those decisions.

A couple of quick reactions, and I want to leave some time for discussion. Some of the cost arguments that we hear against the Financial Services Modernization Act are that the compliance costs will be extremely onerous.\textsuperscript{138} Any time a new regulation goes into effect, there are certainly going to be some compliance costs. If the compliance cost of having regular disclosure and setting up opt-out systems for third-party sharing is going to be so onerous for banks, I think that is very demonstrative evidence that banks have not been adequately dealing with privacy concerns. In addition, there is very strong evidence that there is a great need for strong privacy legislation in the financial services community.

With regard to some of the issues of opt-out versus opt-in, financially savvy Americans tend to believe that their financial information is very sensitive data, indeed. I think we have to take some of the polling data with a grain of salt, as Mr. Howard suggested, because you can find polls that will support almost any position.\textsuperscript{139} I think the only consistent theme that that the polls

\textsuperscript{137} See infra pp. 85-87.
\textsuperscript{138} See supra notes 65-67 and accompanying text.
\textsuperscript{139} See supra p. 94.
evince, namely that the populace is so divided, is great proof that citizens want to be involved. They want to know what is going on with their personal information. But where the issue is financial services data, which the people view as particularly sensitive information, then it does not seem right to put the burden of justifying why one’s data should not be sold and bartered, on the citizen.\(^\text{140}\) It seems perfectly reasonable, on the other hand, that the burden should indeed be on the actor who wants to profit from such information, to demonstrate why he or she ought to be entitled to use it.

Let me address, for a moment, one point that hasn’t come up. Then I want to talk about what I’ll call the sustainability of some of the privacy legislation in the Financial Services Modernization Act.

The first is that part of the attractiveness, I think, for Congress in this statute is to increase the competitiveness of American banks. These are banks that are operating on a global basis. If you look outside the United States, these banks are obligated to comply with far stricter privacy laws than the Financial Services Modernization Act\(^\text{141}\) sets up. So, in effect, what we have set up in the United States is indeed a set of second-class citizens, where Americans will get second-class privacy by the same institutions that are giving first-class privacy to their customers outside the United States.

Now, in terms of sustainability, I think Mr. Howard is absolutely right that there are important constitutional questions that will arise in the context of how the laws and regulations are set up. I part company with that view, however, as to whether it becomes as significant an obstacle to privacy legislation as we have heard about.

The data privacy sphere is very different from the commercial advertising cases that we have seen out of the Supreme Court.\(^\text{142}\) There hasn’t yet been a Supreme Court commercial advertising case that focuses on data privacy and fair information practices

\(140\) But see Esther Dyson, *Control of Private Data Belongs in Hands of Consumers, Not Vendors*, LOS ANGELES TIMES, Mar. 20, 2000 at C3.


\(142\) See cases cited *supra* note 108.
concerns. The commercial advertising cases are all focusing on the solicitations themselves, on the commercial solicitation, and/or the content of the message.\textsuperscript{143}

I think we have to take the \textit{US West} case with a bit of a grain of salt. As a circuit decision, it focused on a number of issues that were different from the pure opt-in/opt-out question: whether the powers were properly delegated to the administrative agency by Congress;\textsuperscript{144} whether Congress had given clear enough marching orders.\textsuperscript{145} If anyone reads the case and reads the docket, I think it is almost impossible not to conclude that the Tenth Circuit grossly misrepresented the factual docket in the case. In deciding that the opt-in rule was unsatisfactory,\textsuperscript{146} the Tenth Circuit basically said the regulatory agency didn’t consider any alternatives.\textsuperscript{147} The point in fact is that the agency had very extensive findings on opt-in versus opt-out that were certainly not addressed by the Tenth Circuit in its opinion.

But coming back to this, I guess you are left with two questions. First, is this commercial speech at all? There is some jurisprudence coming out of the Supreme Court today that suggests there is room to argue that data sales will not be categorized as First Amendment speech. I would point to some language in the \textit{United Reporting v. Los Angeles Police Department}\textsuperscript{148} case and the \textit{Condon v. Reno}\textsuperscript{149} case, even though those were in different contexts. In each of those cases the courts were talking about personal information and the sale of personal

\begin{enumerate}
\item Id.\textsuperscript{143}
\item See U.S. West v. FCC, 182 F.3d 1224, 1228 (10\textsuperscript{th} Cir. 1999).\textsuperscript{144}
\item \textit{U.S. West}, 182 F.3d at 1231.\textsuperscript{145}
\item \textit{U.S. West}, 182 F.3d at 1238-1239.\textsuperscript{146}
\item See \textit{U.S. West}, 182 F.3d at 1238, 1239 (“[T]he FCC’s failure to adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy, indicates that it did not narrowly tailor the CPNI regulations regarding customer approval.”).\textsuperscript{147}
\item Los Angeles Police Dep’t v. United Reporting, 528 U.S. 32 (1999) (holding that California could decide not to give out arrest information, entirely, without violating the First Amendment).\textsuperscript{148}
\item Condon v. Reno, 155 F.3d 453 (4th Cir. 1998) (holding that the Driver’s Privacy Protection Act, which limited public access to information about any individual that was obtained through State’s motor vehicle records, was unconstitutional, as a violation of the Tenth Amendment).\textsuperscript{149}
\end{enumerate}
information, and they were talking about it as commercial or informational products.\textsuperscript{150} If they talk about it as a thing in commerce, then that brings it outside of First Amendment jurisprudence.\textsuperscript{151} So there may be some room to argue that data sales do not constitute commercial speech at all.

If it does not, we go back to the \textit{Central Hudson} test.\textsuperscript{152} There will certainly be, I think, great room for Congress to very clearly articulate why privacy legislation, be it opt-in/opt-out, is justifiable as the narrowest response to the privacy problems identified by Congress. I think that it would certainly be possible for Congress in almost any instance to justify opt-in, just as it would be to justify opt-out.

I think I will conclude on that provocative thought.

MR. MITCHELL: Mr. Reidenberg, thank you for such a boring presentation.

[Laughter.]

Let's give our panelists a chance to come back with any questions or comments. Mr. Ireland, you were the first to speak.

MR. IRELAND: As I sit here, I think the debate is not about privacy. The debate that we are engaged in is related to privacy because that is the instant subject matter. The real issue in controversy here is how do you best solve problems of this nature. Do you best solve them through private market choices, including choices made by individual consumers; or do you best solve it through government solutions?

I have been in the government solution business at least for the last fifteen years, and every year I am more in favor of private market choices. I look at the European privacy principles and I look at this statute, and frankly, as an individual, I wouldn't rely on either one of them to protect my privacy. I have always assumed that any transactions I made with a check or a credit card would

\begin{footnotesize}
\begin{enumerate}
\item See id. at 463; see also Los Angeles Police Dep't., 528 U.S. 32 (1999).
\item See Los Angeles Police Dep't., 528 U.S. 32; see also Condon, 155 F.3d 453.
\item See \textit{Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York}, 447 U.S. 557, 567-71 (1980) (holding that a statewide ban of commercial advertisement by electric companies, where the advertisement in question was not false or illegal, was unnecessary and over-inclusive to carry out the state's goal of conserving energy and therefore violated the First Amendment, even if the company in question operated a monopoly).
\end{enumerate}
\end{footnotesize}
become known to the person I least wanted them to be disclosed to and have conducted myself accordingly.

But really, the tension is do we establish a set of sort of "one size fits all" rights, which is what you do when you do it by legislation, or do you let the market sort itself out? This issue came up at a time of increasing sales and dissemination of information in the marketplace. There is a certain lack of consumer information about what my economist colleagues call "market transparency." What we didn't have was a period of time for that kind of transparency to develop and for consumers and financial institutions to establish their own solutions to these problems.

If you listen to Mr. Howard's polls, there may be a financial institution that fits each of those consumer's desires, his profile, and the people to whom he wants to be marketed. Maybe the best way to do that is for the consumer to choose with whom to do business. If the consumer does not know what the financial institution is going to do with his or her data, he can ask. If he or she is given misleading information and something different is done with the information, he or she can look to traditional common law remedies for fraud, as well as state unfair and deceptive practices statutes, which may apply.

So I think you can talk about privacy, but the real tension is faith in governmental solutions.

MR. MITCHELL: Mr. Soloway?

MR. SOLOWAY: I would just comment on one point that Mr. Reidenberg made that struck me. I think it is somewhat unfair to conclude in any way that financial institutions have not been recognizing and taking care of the privacy concerns and the privacy and data-sharing issues of its consumers, customers, or citizens simply because it has yet to spend anywhere from $10 to $30

---


154. See supra pp. 94-95.

million per institution to comply with the new set of rules and standards that were arbitrarily imposed by the government.

The fact that we haven't met those particular methods, approaches, or criteria does not mean that individuals have not been receiving the privacy protection that is appropriate for them. In particular, when we looked at our own institution and went back and checked our complaint records and so forth, we found nonexistent or minuscule complaints relating to privacy, data sharing, and anything else. In most cases, even when we categorized them as such, they turned out to be more of an inquiry than a complaint.

Now, having said that, I recognize that I will anticipate a lot more complaints forthcoming now that the issue has been brought to the forefront, and the rhetoric surrounding it has, I believe, scared people into concerns that may not be warranted - in particular, a concern that is being posed by the government in its own standards.

MR. HOWARD: I would like to try to respond to three questions that have been raised.

We heard the question, why should we put the burden on the customer when what might make more sense is to ask the person who wants to use the data to justify the use they want to make of it.156 I think the simple answer is found in something that I suggested in my opening remarks,157 and that is that government ought to use the least intrusive remedy that it can to get the desired results. You can always hypothesize an extremely thorough remedy that will absolutely get the desired results, but it will also have very high costs. We have at hand remedies that are relatively lower cost, like disclosure and opt-out, whereas opt-in is a remedy that is pretty expensive in the grand scheme of things.

We might hypothesize for the economy as a whole that it would be good to let the government make all decisions for us in the economy because the government will always have consumers' interests in mind. We have chosen in our country not to go down that road because we think that the free market is better at allocating resources than the government is, and, when we do have

156. See supra p. 103.
157. See supra pp. 89.
government regulation, we try to make it the least intrusive government regulation that will achieve the result that we desire. This goes back to this continuum of remedies thought.

We also heard the question, "Will we become second-class citizens as compared to the Europeans, since they are in some respects using an opt-in regime?" If you think of privacy as an absolute right and think that it trumps all other rights or that no other rights are relevant, you can certainly conclude that you should have maximum privacy protections.

If you want to look at it in a somewhat broader context, you might ask yourself, "Well, what do U.S. economists think about Europe generally?" I think that U.S. economists generally think that Europe is over-regulated and under-competitive. If you go to England, just to pick the European country that is the closest to the United States, I think you could probably get a consensus that people in England have a lower standard of living compared to people in the United States. That is, I would suggest, not an accident. It is the result of being over-regulated and under-competitive.

Some ask whether it is a nice thing to make employee lay-offs difficult. If you consider only the short-term interests of those employees, the answer is yes. It's a very friendly thing to do to make it hard to lay off employees. If you ask, "What has it meant for the European economy to make it difficult to lay off employees as compared to the U.S. economy," I think the answer is fairly obvious. The U.S. economy is far more vibrant than the European economy for just that reason.

Finally, on the US West case, we have the question: is data

158. See supra p. 103.

159. See generally Roger Blanpain, Toward a New European Corporatism?, 20 COMP. LAB. L. & POL'Y J. 497 [hereinafter Blanpain] (noting the European Central Bank’s efforts to crack overregulated national markets on the continent).

160. See e.g., MGMT REV., Oct. 1, 1999, at 42 (discussing the role of the United States in the global economy and stating “[o]nly fourteen percent of the U.S. workforce is unionized today, down from twenty percent in 1983. Other industrialized nations tend to have higher rates of unionization. This provides a high degree of labor market flexibility in the United States, an important spur to productivity and competitiveness.”).

I think that's an interesting question. On the other hand, what is at issue in US West is a narrower question. The issue in US West is whether that company can talk to its own customers. I think that is certainly commercial speech. That is what the FCC tried to essentially prohibit in US West with an opt-in remedy. I would suggest — as I have before — that this is very close to a prohibition.

If you think about the logical result you get if you go down the privacy absolutist road, — if you really believe in the privacy absolutist viewpoint, — you will find yourself wanting to cut off the companies’ ability to talk to their own customers. That is certainly commercial speech and is protected by the First Amendment. I would like to hear a counter-argument to that.

MR. MITCHELL: Joel, we've got to keep it quick. We have to throw it open for some questions. But you have a right to rebut.

PROFESSOR REIDENBERG: Actually, I was going to answer a couple of other points that came up. I think it is unfortunate to demonize privacy legislation. To call it “arbitrary” is surprising, especially since Chase was one of the first banks to endorse the OECD Guidelines that would require transparency.

Mr. Ireland, hit it on the head. Is it a question of regulation and rights, or is it a question of letting the market do what the regulations hope to achieve? Industry, the financial industry, as well as many others, has been very effective in stonewalling any privacy legislation, by saying, “Let us give it time to let the marketplace sort it out.”

I'll give you an exercise to do when you get home today. Get the five different pieces of junk mail in your mailbox. Call the company and try to find out where they got your name and what their privacy policy is. I will bet that on the first phone call you will be unsuccessful. You will have a real hard time finding that out.

One of the banks in this room — I won't name the bank —

162. See id.
163. Id.
164. See supra pp. 82-83.
165. See supra p. 73.
166. See supra pp. 70, 83-84.
sent me a solicitation last year for a financial product and highlighted in the letter was the following statements: "We protect your privacy. We make a commitment to your privacy." I called the bank's 800 number and asked how I could get the privacy policy. "What privacy policy?" was the answer. I said, "Well, it says so in the letter." They asked, "Are you a customer?" I said, "No. I'm interested in deciding whether I want to be a customer. How can I get your policy?" The answer was, "we can't give it to you unless you're a customer."

The marketplace does not work here. It simply hasn't worked and it is not going to work. What we see is that there is a tremendous financial incentive to use the personal information, get as much of it as possible and profile it as much as possible. However, there is no financial incentive thus far, to completely inform the citizens about what is happening. I don’t think it's a question of privacy absolutists or not. I think all of the privacy laws are looking to balance what is the appropriate participation of citizens in the use of their personal information.

Looking at Europe, sure, Europe is over-regulated and has a lot of economic problems. It is not because of privacy legislation. There are things in the European Privacy Directive I would never want to see in the United States. However, there are things in that Directive that we are foolish not to adopt.

MR. MITCHELL: Thank you.

Any questions from the audience after hearing some of our initial skirmishes here?

QUESTIONS & ANSWERS

QUESTION: Where is the role of transition in a regulatory environment for the financial industry? I illustrate that both with the affiliates and the third parties.

On the affiliates side, the worst abuse that I have seen is the bank giving information to its brokerage affiliate. This is the

167. See Blanpain, supra note 159 and accompanying text.
168. Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Art. 32, 1995 O.J. (L 281) 31 (requiring Member States to adopt legislation conforming to terms of Directive).
s...
My colleagues at the SEC would be apoplectic, because you have described somebody who is bamboozled by the broker and sold some inappropriate investment, which is a violation of their sales practice rules. They have a regime that they at least are very proud of, which they think provides a remedy for that problem. So, to the extent that you have a problem in that area, it is not that the information was disclosed. It is that they were sold a bad investment.

What if they were sold a good investment? What if they left the bank and the bank said, “We pay you; you’ve got a money market with us, and we have to pay deposit insurance against that. We have to comply with all those banking regulations, and we hold reserves against your checking account and so on. We can offer you a money market fund that is not a deposit but is invested in a government securities mutual fund that is not insured and is going to pay you two percentage points more.” Do you want that? Maybe they just got a whole lot better deal by virtue of cross-marketing. You don’t know. It’s case-specific.

One way to go about this, — the argument that was made in the congressional process — is since banks are expanding affiliations and are going to be dealing with more people, we should start now. The other argument is, “We don’t know what is going to happen. Why don’t we do what we set out to do, allow greater affiliations, and then wait and see if that creates a problem?” Again, it boils down to where your faith is. Is your faith in the market system, or is your faith in the government deciding what the rules are? My own view, somewhat like Mr. Howard’s, is that the 20th century was not terribly kind to planned economies.

MR. MITCHELL: I want to thank our panelists for coming. Fordham University Law School thanks you. We all enjoyed it.