Some Practical and Theoretical Thoughts about Privacy and Banking

Julius L. Loeser

When Comerica Bank earlier last year distributed privacy principles to its retail customers and gave them the right to opt out from information sharing, it not only gave them the right to opt out from information sharing with affiliates, which most banks have done, but it went further and also gave them the right to opt out from sharing of information with third parties, which is what the Gramm-Leach-Bliley Act now requires.

EXPERIENCE WITH THIRD-PARTY OPT-OUT

Our experience, admittedly in a "pre-U.S. Bancorp" environment when privacy in banking did not have as much notoriety as it does today, was that less than 1 percent of the customers opted out. However, the intensity of the feeling of the people who did opt out was considerable. The word "appalled" or a variation of it was in virtually every letter, *i.e*. customers were appalled that a bank would consider transferring customer information to other parties.

I believe that illustrates a need for banks to communicate to their customers that there are innocent transfers of information, such as to printing firms for the preparation of statements or to facilitate a merchant's acceptance of a check written by the customer; that banks generally maintain customer information confidentially; that when information may be transferred to third parties for marketing purposes details of customer transactions are not transferred; and that there can be benefits to permitting transfer of information to third-party marketing firms. Some of those benefits are discussed below.

MORE SIGNIFICANT INTRUSIONS

It is ironic that, while what I sense are antibusiness interests criticize bank sharing of information, they seem oblivious to much greater threats to personal privacy emanating from government intrusion. Banks are required by federal law to file currency-transaction reports with the government whenever a customer engages in a transaction using $10,000 or more (in some geographic areas, as little as $3,000) in cash.[1] Banks are also required by law to keep records of wire transfers and to disclose those records to the government on request. Banks are required to file reports or keep records of purchases of money orders over a certain amount and are also required to file suspicious-activity reports whenever they observe anything suspicious on the part of any of their customers.

Under a recently adopted rule of the US Department of Health and Human Services (HHS) that is known in the industry as "Data Match" and is intended to help the government locate "deadbeat parents,"[2] HHS periodically will deliver to banks lists of "deadbeat parents," *i.e.* parents who are not paying child support. Banks are to deliver to HHS or its agents a computer tape listing their account holders so that the government can garnish the funds in any corresponding accounts. Alternatively, a bank may compare HHS's lists against its list of depositors and report to the government any accounts held for persons on the lists, thereby preserving the confidentiality of most of its customers. Most banks are delivering their customer lists to HHS, as this is a less-costly way of complying with this requirement.

AFFILIATE SHARING

Ironically, privacy activists do not appear to focus on intrusions like "Data Match," yet focus not only on third-party sharing, but also even sharing of information among affiliates. From the perspective of any business, the concern over affiliates sharing information seems particularly misplaced. The very existence of affiliates often is an accident of corporate structure. The way a corporate organization is structured is a function of a number of variables unrelated to information sharing, including tax laws and

even personalities, as an executive may wish to be CEO of his or her own operation so that a business is set up as a separate affiliate. In a perfect world one might merge all affiliates together into a single corporation which would eliminate any affiliate-sharing issue whatsoever. However, because of vagaries of corporate structure, an affiliate-sharing prohibition would block the flow of information in an organization, because of the accident of corporate structure.

BENEFITS OF THIRD-PARTY SHARING

IBM Corporation recently has televised two commercials that, intentionally or not, illustrate some of the benefits of third-party information sharing. In one, a gentleman in a focus group complains, "I get catalogues for toys, and I don't have kids." Why does he get catalogues he does not want? It is because no business has shared information about him with the toy-catalogue issuer enabling the catalogue issuer to target market, and so he receives unwanted catalogues for toys. A second person responds, "I get discount coupons for car repairs, and I take the subway." Again, businesses have not shared information about this person and so a marketing firm has been unable to target market, and thus this second person receives nuisance marketing communications. A third person adds, "I get calls for aluminum siding, and I live in an apartment." Again, failure to share information has led to needless intrusions into a consumer's private life. Someone then turns to the two-way mirror from behind which the focus group is being observed and angrily shouts, "You've got all the databases in there, but you don't know who we are." This television commercial illustrates one of the benefits of permitting sharing of information. It spares people from unwanted, potentially intrusive marketing efforts.

The second commercial highlights another information-sharing benefit. In it, a pair of grocery-store clerks is cleaning up late at night, and one picks up what apparently is particularly odoriferous cheese and comments on the smell. The other asks, "Who buys that smelly stuff?" The omnipotent voice of the off-screen store manager, who apparently, with the viewer, is sitting

in an office above the store watching, responds over a loudspeaker, "The people who buy that smelly stuff also buy 90 percent of the baby vegetables over in produce. Have you ever looked at the markup on baby vegetables?" This illustrates another benefit of what some might consider an intrusion into personal privacy, *i.e.* tracking what particular individuals buy. A store's ability to track who is buying what, and what other things they buy, enables the store to meet customer wants and to increase profits, in theory potentially even to lower prices. This is precisely the benefit of supermarket discount cards. Such cards provide discounts to customers who permit their purchases to be tracked by the issuer, enabling the store to learn that customers who buy smelly cheese also tend to buy baby vegetables.

A free-market economist might observe that, if a business wishes to share information from customers, it ought to pay customers for that information or for the right to share that information. That is exactly the case with supermarket discount cards. Supermarkets are paying people for being willing to sell information. The supermarket will give a customer a discount on its products because the customer is willing to let information be collected.

That theoretically raises a question about the new legislation under which banks have to give consumers the right to opt out. Following the lead of supermarket discount cards, might a bank increase deposit interest rates or reduce loan fees for customers who do not opt out? If that would be permissible, could a bank conversely increase prices to people who opt out? In essence, that is what grocery stores are doing.

BEYOND BANKING

While, for some reason, policymakers concerned about privacy have focused on the banking industry despite its long tradition of customer confidentiality, the new privacy legislation applies to many other industries as well. It applies to any business engaged in activities in which banks or their affiliates will be permitted to engage under the new law. Under the new legislation, that includes businesses as varied as real estate

development and wire transfer, automobile dealers that finance cars, department stores and other retailers that issue credit cards, as well as stock brokerage firms, insurance underwriters and agents, and even travel agencies. Businesses in each of those industries will be required to adopt privacy policies and provide them annually to customers, to permit their customers to opt out of information sharing with third parties, and then to track those who have opted out.

"MARXIST" ANALYSIS

To the extent that, as discussed above, one of the customer benefits of sharing information is to facilitate target marketing and thus spare consumers the nuisance of receiving marketing communications in which they would not possibly be interested, one might see a clash of two competing, admittedly ill-defined, consumer-interest groups when it comes to the issue of privacy; *i.e*. the interests of those who wish to be marketed for products and services in which they might be interested, but who do not wish to be bothered by marketing solicitations for unwanted products and services, clash with the interests of those who want to prevent information sharing because they see it as an intrusion upon their privacy.

A recent National Public Radio broadcast presented what I think of as a class-warfare, almost Marxist, analysis of these types of competing interests. It reported that some argue that impeding the free flow of marketing information to customers informing them of the availability of products and services they desire hurts low-income persons. The premise is that, while the rich have ready access to information about products and services, perhaps through the Internet or by subscribing to *Consumer Reports*, the poor do not have such ready access to information about products and services and cannot afford to purchase such information. Under this analysis, it is thought that lower-income persons therefore benefit most from targeted marketing that information sharing facilitates, and, thus, those who would impede information sharing are advocating a course of action that would harm the less fortunate.

THEORETICAL THOUGHTS

The Fifth Amendment

The premise of privacy advocates is that information about a person is a property right of that person. However, information that one person gleans about another person based on the former's experience with, or observation of, the latter can hardly be deemed a property right of the latter, but may well be a property right of the former. Admittedly, it may be a different issue whether information about someone given to a business by the person who is the subject of the information remains the property of the person or becomes the property of the business; however, it is not absurd to argue that a recipient of information from a person who is the subject of the information, absent some other contractual understanding with the giver of the information, acquires a property interest in the received information. In either case, a constitutional issue would appear to be raised whether legislation restricting the use of the information that is property constitutes a Fifth Amendment "taking."

The First Amendment

There may also well be First Amendment issues that need to be considered in this area. Some states have prohibited the release of arrest records to persons who would use the records for commercial purposes (*e.g.* publishers, attorneys, insurance companies, drug and alcohol counselors, religious counselors, driving schools) while permitting the release of such records for other purposes (*e.g.* scholarly, journalistic, political, and governmental). This may not be substantially different from the Gramm-Leach-Bliley Act's permitting the sharing of customer information for many purposes (*e.g.* to bank regulators, law-enforcement agencies, and judicial authorities) as well as admittedly for some commercial purposes (*e.g.* servicing, securitization), but not other commercial purposes. (Note the act's paternalistic prohibition against sharing account numbers for use in marketing, even with the consent of the customer.)

Some federal courts have held that, in enacting arrest-record statutes like those described above, state legislatures have drawn

a line based on the "speech use" of such records, disallowing release to those wishing to use them for commercial speech, while allowing their release to those having a noncommercial purpose. One example of such a ruling is *Lamphere & Urbaniak v. Colorado*, 21 F.3d 1508 (10th Cir. 1994). (In my analogy to the Gramm-Leach-Bliley Act, the person whose free speech is being infringed might well be the third-party marketing firm from which the information is being withheld, not the free speech of the bank holding the information.) Such courts have gone on to conclude that, because commercial speech is protected under the First Amendment (albeit less than "core" First Amendment speech), and because speech includes direct-mail solicitation (Q: even the despised telephone solicitation?), the restriction constitutes a content-based restriction on protected speech. See *Speer v. Miller*, 15 F.3d 1007 (11th Cir. 1994).

A similar principle was invoked when the state of Minnesota imposed a use-tax on paper and ink only on producers of periodical publications. See *Minneapolis Star & Tribune Co. v. Minnesota Commissioner of Revenue*, 460 U.S. 575 (1983).

More pertinent is *U.S. West, Inc. v. Federal Communications Commission*, No. 98-9518 (10th Cir., August 18, 1999) which held that it is not permissible to curtail commercial speech unless it is to protect substantial rights and the protective measure is narrowly tailored. In that case, the Federal Communications Commission had adopted regulations requiring customer opt-in before telecommunications firms could lawfully share information concerning to whom, when, and where a customer places a call. The regulation implemented a provision in the Telecommunications Act entitled "Privacy of Customer Information." The 10th Circuit held that the commission failed to consider adequately the First Amendment.

In discussing the First Amendment issues, the court stated that, for the government to be found to have the requisite substantial interest in privacy to pass First Amendment muster, it "must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals." The court questioned whether undue embarrass-

ment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purpose of assuming another's identity give rise to a sufficiently-substantial interest. The court also suggested that an opt-out procedure is more narrowly tailored than an opt-in procedure and, thus, more likely to withstand First Amendment scrutiny.

LOOKING FORWARD: THE NEXT PRIVACY-POLICY DEBATES

Privacy activists believe that, not only should a consumer be able to control the use of data about that consumer, but also the consumer should have a right to correct erroneous or incomplete information about him or her, and that requires access to the data by the consumer. Certainly, this policy is codified in the Fair Credit Reporting Act in areas in which the availability of credit, insurance, and employment may be affected by information. It is not clear that there is a similar compelling need to ensure information accuracy in the area of marketing, however. Nonetheless, the Federal Trade Commission must think that the need to ensure accuracy of information for marketing purposes is fairly compelling, as "access" is one of five information principles it has adopted. The Department of Commerce, in negotiating with the European Union, also has established access as a requisite element in a program that meets the requirements of the EU directive prohibiting a member country from permitting the sharing of information with persons in any other country that does not have adequate privacy protections in place. The business community, perhaps predictably, normally does not provide access because of the costs involved.

Undoubtedly, the next frontier in the privacy debate will be state legislatures. The Gramm-Leach-Bliley Act reserved authority to states to legislate in this area, and various state attorneys general have been active in pursuing what they deem to be misuses of customer information by banks. Legislation is already pending in some states, and legal scholars are already debating whether the Fair Credit Reporting Act, which permits information sharing with affiliates in cases in which customers have been given the opportunity to opt out and not done so, may

preempt any state laws that are eventually enacted purporting to restrict affiliate sharing.

THE BIGGER PICTURE

Finally, it would not be proper in closing a piece such as this to fail to take a step back and consider the bigger picture, and that is how the banking industry is very cognizant that what sets it apart from other financial-services industries is the trust that it has engendered from customers. Bankers realize and, in their cloistered conversations about policymakers' sudden, new-found interest in privacy, often dwell on the fact that the basis of the customer trust the industry enjoys is that, for many decades, the industry has guarded the privacy of its customers. It is not idle bombast to say that, over the years, the banking industry has led American business in protecting customer privacy and expects to continue to do so.

Notes

[1] 31 CFR 103.22.
[2] 42 U.S.C. 666(1)(a)(17)(A).