Privacy Issues Proliferate in the 21st Century

Alvin C. Harrell, Oklahoma City University School of Law
month period but must apply it consistently. For instance, the institution may define the period as a calendar year and then must provide the annual notice once each calendar year following the calendar year in which the initial notice was given.

The annual notice must be provided by mailing a copy to the customer's last known address. For joint accounts, one annual notice (during each period) may be provided jointly.

Financial institutions are not required to provide the annual notice to former customers. A customer becomes a former customer with regard to closed-end loans when the loan is paid in full, charged off, or sold without the retention of servicing rights. For mortgage brokers, a customer is a "former customer" after the customer has obtained a loan or has ceased using the mortgage broker. In cases where there is no specific time at which the customer relationship terminates, the customer becomes a former customer when the financial institution has not communicated with the customer about the relationship for 12 consecutive months (other than to provide annual privacy notices or promotional material).

The content requirements for the annual privacy notice are the same as the requirements for the initial privacy notice.

G. Revised Privacy and Opt-Out Notices

Revised privacy notices are required when an institution wishes to disclose nonpublic personal information to a nonaffiliate other than as described in the initial notice. A new opt-out notice is required and the consumer must be given a reasonable opportunity to opt out prior to disclosure. The new privacy notice is required if there is a new category of information to be disclosed, if there is a new category of a nonaffiliate, or if disclosure is to be made about a former customer who did not have the opportunity to opt out. A new notice is not required to disclose information to a new nonaffiliate adequately described in the prior notice.

V. Conclusion

The privacy provisions of the Gramm-Leach-Bliley Act and the implementing regulations require careful analysis of the entity's privacy policies. This analysis will enable the entity to implement the appropriate notices to consumers and customers. Covered entities include a wide variety of non-banking enterprises that are now within the broad expanse of the term "financial institution," including possibly some law firms. For some of these enterprises, the transition to the new world of customer privacy may require some difficult and fundamental adjustments. Welcome to the new world of "financial institutions."

Privacy Issues Proliferate in the 21st Century

(Continued from page 2)

The government has a monopoly on the legal use of coercion, and this sometimes breeds a lack of sensitivity on the part of those who represent the government and exercise its authority, particularly if there is a public policy "war" against something going on, which there frequently is. Private entities are not immune to this, but in contrast rely on voluntary transactions and custom goodwill for the entity's very existence, and therefore tend to be more responsive to customer preferences. No amount of alleged "market power" can change this basic distinction. This is not to suggest that private companies always do the right thing, but merely that government agencies sometimes do not. The public seems generally to recognize this danger.

So it may seem surprising that virtually all of the recent legislative and regulatory initiatives have been directed exclusively at protection against private parties. Indeed, there are clearly new pressures for expanded federal access to private information in the aftermath of the September 11, 2001 terrorist attacks on the Pentagon and World Trade Center. While understandable, this increased emphasis on restricting the private use of business records while expanding the government's access to private information represents a reversal of traditional American priorities. As with some other issues, this new focus seems to be driven partly by changes in technology that are perceived to be creating new issues relating to consumer privacy expectations.

The more efficient use, storage, and transmission of data means that more consumer information can be assembled and accessed in usable form than in the past. Indeed, the gains in this respect are so dramatic that a respectable body of opinion now holds that informational privacy in the modern age is an illusion, and that any legal barriers to the use of data will inevitably be ineffectual as to constitute mere window-dressing for public consumption.

(Continued on page 4)
cedures in place to appropriately handle customer data under the myriad of laws affecting privacy and disclosure. The following is a possible checklist for analyzing the treatment of information sharing under the FCRA, RFPAs and the GLB Act:

1. Whose information is being shared?
   - If it is consumer (personal, family or household use) or customer information: The GLB Act and the FCRA apply.
   - If a business, is it a proprietorship or partnership with five or fewer individuals? If so, the RFPAs apply.

2. What kind of entity is seeking the information?
   - If a government agency, is it federal (RFPAs may apply) or state (check state law)?
   - If a government agency, is it a tax collector? If so, special rules may apply.

   - Is it an affiliate (check the definitions in both the GLB Act and the FCRA)?
   - Is it a joint marketer? (If so, is there an agreement to keep the information confidential?)
   - Is it a third party?

3. If the entity is a third party, does it fit one of the GLB Act exceptions? If not, has the institution satisfied the GLB Act requirements of notice and opt-out opportunity?

4. Is the request for records involved in a civil or criminal court proceeding? If a grand jury proceeding, note any requirements to keep the notice confidential.

5. If there is either a court proceeding or agency involved, did the institution receive a summons or subpoena that was properly served? If RFPAs apply, was there a proper notice to the customer? Request a certificate of compliance! Note the importance of beginning to collect the records to satisfy the time requirements of the request. Keep careful records of time and the costs for reimbursement purposes where available. Do not go beyond the scope of the records request.

VIII. Conclusion

While “dot com” companies and direct marketers are receiving a great deal of adverse publicity right now over information sharing, there are many legitimate ways to share information with third parties. More significantly, there are many laws requiring information sharing with various government agencies for both civil and criminal matters. Furthermore, the last line has not been written yet as Congress and state legislatures revisit privacy in the months and years to come. All of the indications are that this will be a significant and expanding area of law for providers of financial services for many years to come.

---

Privacy Issues Proliferate in the 21st Century

(Continued from page 22)

Technology has caused other privacy issues and challenges. Internet privacy has become a field of its own covering not only information voluntarily provided by Internet users, but data scrubbed involuntarily via “cookies” and similar devices, not to mention hackers. Other forms of identity and information theft create additional issues. Telemarketing fraud (and inconvenience) are also problems with privacy invasions. The war on terrorism is a major new factor.

Many consumers seem to draw distinctions between financial records, medical records, and other personal information. Consumer credit reports have always been available, and many consumers recognize that the widespread availability of this personal financial information enables them to conduct financial transactions with strangers. But personal medical information often strikes a different chord. Similarly, many consumers appreciate the informational benefits of cross-marketing and targeted marketing efforts, while others do not.

Many economists emphasize that an information economy runs on data, and to cut off that data would have serious economic implications. Clearly there are correlations between a free flow of information and economic productivity and prosperity, not to mention basic human freedoms. This is not to say that restrictions on private information are always good or bad, only that the economic and human costs of such restrictions, and their likely effectiveness, are legitimate considerations which deserve attention by policy-makers and the public.

II. The EU Directive

The European Union (EU) Data Directive was adopted in 1995 with implementation to be achieved (by national laws of member countries) by 1998. It requires unambiguous consent prior to transfer of personal data to third persons, and bans export of such data to countries with inadequate data protection systems. Under the EU standards, the U.S. is an inadequate protection jurisdiction and is therefore ineligible to receive EU data. This essentially prohibits transmission of data from the EU or to the EU from the U.S., or the processing of EU data in the U.S. The various exceptions are generally deemed ineffective and unsatisfactory. An enforcement moratorium expired July 1, 2001.

The EU Directive raises again, in an international context, many of the issues noted at Part I above. It is said by critics to be unworkable, inel-

2. Directive 95/46/EC (1995). See generally Ruth Hill, Ross Brian, Horsham and Mark Winton, And We Thought KMCA was (Continued on page 70)

QUARTERLY REPORT

XXII. Usury

In Cohen v. Eisenberg, the plaintiff committed to make a $120,000 “hard money” mortgage loan to the defendants at 19.5 percent interest. The loan was closed in the name of American Universal Mortgage Banking, Inc. (American) and immediately assigned to the plaintiff. The defendants defaulted; the plaintiff foreclosed; the defendants raised the affirmative defense of usury; and the trial court dismissed the affirmative defense. The appeals court reinstated the defense on grounds that American’s participation in the loan was only to enable the plaintiff to evade New York’s usury law, i.e., American was a “qualified creditor” under DIDAMCA, which allowed it to charge interest rates in excess of the state’s usury limitation, but was not the true lender in the transaction.

XXIII. Yield Spread Premiums

In Glover v. Standard Federal Bank, class certification was granted on yield-spread premium claims on the plaintiffs’ renewed motion, based on the judge’s finding that (1) HUD did not intend by its March 1, 1999 Policy Statement to articulate the less stringent test adopted by other courts in the Minnesota district (and elsewhere); and (2) even if it did, such a test was arbitrary or capricious and, thus, could not stand.

Of course the law in this area was thrown into further turmoil by the latest Calpepper decision, which adopted a surprisingly stringent view of RESPA section 8 in this context. This decision will require careful consideration by anyone utilizing yield-spread premiums in mortgage finance.

All of the cases discussed in this article reflect the varied perils that confront any lender seeking to serve the sub-prime credit market.


Privacy Issues Proliferate in the 21st Century

(Continued from page 45)

ffective and unnecessarily costly. It has been noted that unemployment levels are higher while productivity and economic growth are lower in the EU countries. It has even been argued that the EU Directive is a new form of economic protectionism, designed to prevent EU companies from setting up data processing centers in more modern, lower-cost countries like the U.S.

During the ABA 2000 Annual Meeting in London, your author attended a program on privacy that included advocates of the EU position. During this program it was pointed out that the EU Directive is flagrantly violated in all EU countries, indeed that there is no apparent evidence of compliance in any EU country. The response was that it is necessary to understand how European law works: Governments pass laws that include wholesale restrictions on private activity; corporations then petition the appropriate administrative agencies for formal or informal exceptions on a case-by-case basis. The absence of large-scale consumer litigation means that major enterprises can develop workable arrangements with enforcement agencies that essentially carve out huge exceptions to the law. It is all very anti-competitive, as the exceptions to unknowable laws may essentially constitute an exclusive license to do business, shutting out small competitors that lack the clout to obtain such concessions. But this is apparently the modern European tradition.

This means that “the law” may not really be the law at all, except as to cases where the political authorities want it to be. Sometimes observers may feel that this is the way administrative agencies function in other jurisdictions as well, but in the U.S. at least the importance of private litigation makes it more difficult to ignore plain statutory language. Thus the EU Directive reflects a cultural divide between Europe and the U.S. that potentially affects the essential transmission of data across the Atlantic Ocean in unprecedented ways.

III. Comparison of U.S. Law

In the meantime, privacy law continues to develop very differently in the U.S. In North America the free flow of information, and the freedom of entry for new firms afforded by the common property-based common law systems in most states, engendered a technology revolution that is reshaping the world. The benefits to companies and consumers alike, in terms of lower costs, expanded choice, greater information and expanded opportunities, are manifest.

Contract law continues to be the primary consumer remedy, in spite of comprehensive legislation like the Gramm-Leach-Bliley Act (GLB Act). While the GLB Act rules (and counterparts in some states) seem poorly drafted and unnecessarily cumbersome to many who must work with them, thereby raising costs while imposing unnecessary and (sometimes ineffective) barriers to commercial information flows, to its credit the GLB Act continues the American tradition of relying on disclosure, contract law and private litigation as the primary enforcement mechanism.

In essence the GLB Act requires disclosure to consumers and customers of a company’s privacy policies. While questions of “opt-in” versus “opt-out” approaches raise serious issues, the GLB Act’s primary reliance on contract remedies for consumer redress is far more important. In effect, financial institutions (as broadly defined) must make disclosures pursuant to the GLB Act, but there is no statutory penalty or private right of action in the GLB Act; the primary consumer remedy for a violation will be an action for breach of contract or violation of state consumer protection laws. This relies on the theory that company policies and promises, publicly announced and justifiably relied upon,
D. Enforcement Provisions

A consumer home loan that violates these consumer protections is usurious and the making of such a loan is considered to be an unfair and deceptive trade practice under N.C.G.S. section 751.1, subjecting the lender to treble damages and attorney’s fees. The Attorney General of North Carolina, the Commissioner of Banks, or any party to a transaction may enforce the provisions of N.C.G.S. section 24-10.2. Recoveries for a violation of this section may be obtained under either the provisions Chapter 24 (Usury) or Chapter 75 (Unfair and Deceptive Trade Practices), but not both. Certain fee-shifting provisions apply as to attorneys’ fees.

IV. Study on the Effects of Senate Bill 1149 Commissioned

The North Carolina General Assembly recognized that Senate Bill 1149 would be plowing new ground in the field of consumer protection, and accordingly made provision for the Legislative Study Commission to study the implementation and enforceability of the Act. The study is to include the Act’s impact on the availability of credit and whether the legislature successfully reduces predatory lending practices. The study commission is to give its report to future sessions of the North Carolina General Assembly.

Privacy Issues Proliferate in the 21st Century

(Continued from page 76)

constitute a contract with consumers and consumers. It preserves a paramount role for traditional American legal principles, preserves an important role for state laws, while providing a degree of national uniformity, creates an effective system of private remedies, and permits some flexibility on the part of companies in designing their privacy policies. While we might wish for a better execution, as a policy matter it could be worse.

IV. Critics on Both Sides: Prospects for the Future

Yet the GLB Act has been severely criticized, even aside from its unnecessary complexity and cumbersome nature. From the consumer side comes the usual scare-stories: it seems that every case of identity theft now warrants a newspaper headline and a story demanding greater privacy protections, even though such cases are primarily a problem of crime rather than corporate information sharing. The GLB Act, and most privacy proposals, do little to address identity theft. Indeed, while identity theft is undoubtedly frustrating to its victims, and makes a great headline, it is not clear how pervasive the problem is or even that it is increasing.

Other examples of scare tactics, knee-jerk responses, anti-technology backlash, ill-defined problems and ineffective yet unwieldy proposals continue to proliferate. The risk of unintended consequences is ever-present. Yet privacy, like predatory lending, remains undefined and widely misunderstood. One can only wish that policy makers would define what it is they are seeking to prohibit. The result of this failure is the risk of an economic and legal bonfire without any prospect for a serious public benefit.

As usual the issues are more complex than the public, the media and many policy-makers (and commentators) seem to understand. To be effective, the next stage of public policies will need to distinguish between transactional use of information (which must remain largely unrestricted if the economy is to function freely), information sharing (or sale) and plainly criminal activity. Free and open access to transactional information is essential to credit availability and funds transfer systems. A focus on criminal activities and enforcement should not be allowed to impede legitimate financial transactions. Distinctions may also need to be made between types of information, e.g., financial information may need to be better distinguished from medical information (the latter being deemed more sensitive with less need for widespread availability). To paint with too broad a privacy brush could be disastrous.

The GLB Act deserves credit for its emphasis on the traditional American notions of notice (disclosure) and choice (contract law), and for being a statute that says what it means and is intended to apply equally to all. The lack of a statutory penalty or right of action in the GLB Act preserves the state law remedy structure. It is far preferable to the EU approach. But the GLB Act is not perfect. As with much federal legislation, it is far too complex and difficult to implement, with costs that greatly exceed its minimal benefits. The GLB distinction between information flows to affiliates versus flows to nonaffiliates is logical and perhaps unavoidable, but it favors large conglomerates with diversified affiliates over independent companies. Your author bears no grudge against conglomerates, but this policy bias is unfortunate, even though less pronounced than in the EU.

A major debate is looming over opt-in versus opt-out. Given natural human inertia, opt-in systems (requiring consent for use of information) as in the EU Directive are tantamount to non-use. Opt-out systems at least offer those most concerned the opportunity to act on that concern, with less disruption to others.

If future privacy laws are to effectively make the distinctions necessary to preserve essential
borrower at least three days prior to the closing.

V. Penalties for Violations; Correction of Errors and Good Faith Reliance

A. Civil Penalties

The Banking Department may assess civil money damages against lenders who violate the High Cost Loan Regulations, and is authorized to take other enforcement action, such as revocation of a mortgage license, against others who violate these new regulations.

B. Correction of Errors

A lender or assignee has no liability for failure to comply with any requirement of the High Cost Loan Regulations if within 60 days after discovering an error, whether pursuant to a final written examination report, through the lender’s or assignee’s own procedures, or through a complaint from the obligor, and prior to the institution of an action under the regulations, the lender or assignee notifies the individual(s) concerned of the error and makes whatever adjustments are necessary to either correct the error or assure that the person will not be required to pay an amount that will render the loan a high-cost home loan.

A lender or assignee has the right to correct errors and may not be held liable for a violation of the High Cost Loan Regulations, however, only if the lender or assignee shows by a preponderance of evidence that the error was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adopted to avoid any such error. Examples of bona fide error include, but are not limited to, clerical, calculation, computer malfunction, programming, and printer errors, except that an error of legal judgment is not a bona fide error.

C. Good Faith Reliance

A lender or assignee may not be held liable under the High Cost Loan Regulations for any act done or omitted in good faith in conformity with any rule, regulation, release, bulletin, or interpretation issued by (i) the Banking Department, or (ii) with respect to provisions of the High Cost Loan Regulations that follow the Federal Truth in Lending Act, the Federal Reserve Board.

VI. Other Significant Provisions

A. Multiple Borrowers

Where there is more than one borrower on a high-cost home loan, and the High Cost Loan Regulations require a notice to be given or a signature obtained, such requirement will be deemed satisfied if the delivery or placing in the mail to, or obtaining the signature of, any borrower who is primarily liable on the high-cost home loan.

B. Legend

High-cost home loans must include a legend on top of the mortgage in 12 point type stating that the mortgage is a high-cost home loan subject to Part 41 of the General Regulations of the Banking Board.

Privacy Issues Proliferate in the 21st Century

(Continued from page 85)

information flows while combating abusive practices, they will have to be even more complex and certainly more finely crafted than the GLB Act. The probability of a successful execution of these goals cannot be regarded as high. The potential costs and risks of unsuccessful forays in this policy area are thus significant. Privacy initiatives therefore may be regarded as a serious potential threat to the continuing expansion of the information economy. Privacy burdens and complexities more onerous than the GLB Act could have a dramatic and disproportionate impact on the competitiveness of American businesses of all types, both large and small.

The knee-jerk reaction to any perceived problem, by many in the public sector, media and public, is to pile on reams of new laws, rules and regulations without any serious consideration of the costs or benefits. Consumers may not see these costs, buried in the prices and availability of goods and services, but consumers certainly will pay them. If these laws increase costs, generate useless litigation, reduce economic competition and employment by imposing undue burdens on small businesses, and yet provide no significant benefits, then society will have made another bad public policy bargain.

Two final, related points deserve mention. First, it is possible that the detractors of all privacy legislation are correct in their view that efforts at a legal solution are futile; information flows are so pervasive that short of an old-fashioned police state there may not be any effective way to restrict personal information and still allow the system to operate. In other words, legal privacy protections may be largely a myth, here and abroad, no matter how many rules and disclosures are issued. Second, the answer may be technology, not law. Technological solutions that allow individuals and companies to better safeguard the privacy of their information offer some hope of enhanced data protection in the future, regardless of the law. This may offer the best prospects in the context of a free and open, contract-based legal system that does not seek to restrict all information flows on an arbitrary, system-wide basis.

3. A paradox of modern society is that improved technology in conjunction with a sophisticated legal and political culture is producing complex, intractable legal solutions to a large range of perceived problems, to the point that this complexity itself has become a problem. A political tendency to consider each problem in isolation, without adequate consideration of the impact of proposed solutions on the context of other issues, adds to the confusion. The resulting complex legal environment challenges the kind of simple, individual solutions that have been a hallmark of Western progress for 1,000 years. Some believe the impact could be dramatic. See, e.g., Robert S. Boyd, Parts of Whole: May Be Headed toward Death, Scholem's Step- gest, Phil. Inquirer, Mar. 25, 2001, at A12 ("Complex societies have been collapsing for 12,000 years—as long as they have existed."). Adding numerous finely crafted layers of complex requirements may seem appropriate to lawyers engaged in the front-running process, but at some point the result may become unworkable for the average citizen and business who must use the system.