Marquette Elder's Advisor

Volume 3
Issue 3 *Winter*

Article 9

Privacy and Pension Plan Records: Is Self-Regulation Sufficient?

Michael J. Francis

Privacy and Pension Plan Records: Is Self-Regulation Sufficient?

The confidentiality of employees' pension information is being threatened by changes in the design of qualified retirement plans and advances in data-processing and Internet technology. Despite the passage of recent laws aimed at protecting privacy, more may need to be done to ensure that personal financial information remains secure.

By Michael J. Francis

The idea of a trusted financial-services organization selling information regarding your retirement savings balance and investing habits to the highest bidder would be enough to get most people writing letters to their congressmen. Yet this is a real possibility, given the lack of meaningful privacy protection for the extremely sensitive financial data maintained by retirement-plan service providers and the significant financial incentives these providers have to share personal financial information with affiliated and third-party marketing organizations.

This article explores how changes in the design of qualified retirement plans, advances in data processing technology, and the Internet combine to put the confidentiality of employee retirement plan information at increasing risk. Despite laws recently passed by Congress designed to protect sensitive financial information individual's retirement savings information remains unprotected by these laws. While profiting from the sensitive financial information of its customers is not currently a common practice among those in the business of handling retirement plan records, a review of several providers' service agreements reveals an industry determined to keep its options open.

Retirement Plan Background Information

Retirement plans arose from corporate America's desire to retain long-term employees, discourage the formation of unions, and provide a dignified exit for older employees, thereby allowing for their replacement by younger and less expensive workers. Over the first one hundred years, however, a number of corporations made promises to employees that were not kept. Notably, Studebaker Corporation defaulted on its pension plan obligation in 1963, an action that is thought by many[1] to be the catalyst that led

Michael J. Francis has spent the past eighteen years in the financial-services industry and provides consulting services to numerous qualified retirement plan sponsors. He received a J.D. degree from Marquette University Law School in May 2001.

to the passage of the Employee Retirement Income Security Act of 1974 (ERISA).[2]

ERISA's pension plan reforms were primarily inspired by Congress' desire to safeguard American workers' retirement assets, and motivate employers' increased use of pension plans.[3] But ERISA's increased compliance demands unintentionally drove many employers to terminate plans that guarantee retirement benefits, so-called "defined benefit" pension plans, in favor of "defined contribution" pension plans (e.g., profit-sharing and 401(k) plans). Because they shift much of the risk of funding retirement benefits onto employees, defined-contribution plans have rapidly surpassed defined benefit plans as the most prevalent form of retirement benefit today.[4]

The shift from defined benefit plans to defined contribution plans has important implications for the privacy of personal financial information because of the different type of records available from each type of plan. For defined benefit pension plans, the only financial data that is typically available to participants is the monthly income benefit available at retirement age. Defined contribution plans, on the other hand, keep individual participant records much like a bank. Money is deposited into an individual's account, by either the employer or the employee, and is invested. With all this activity, defined contribution plans can contain a significant amount of highly sensitive financial information such as current retirement assets, savings percentage, risk tolerance level, loan amounts, investment strategies, and beneficiary information.

Not only does the move towards defined contribution plans make more data available, but the accelerating pace of technological advancement makes this data increasingly accessible. As recently as the early 1980's, major corporations kept retirement plan records on three-by-five note cards and participants received updates once a year. Today, thanks to improved data processing capabilities, most participant data is updated daily and is instantly retrievable on the Internet. This makes it profoundly more cost effective for sensitive financial information to be retrieved and exploited.

Finally, with the average participant account value estimated to be over $50,000,[5] the potential gains to a financial services organization from the successful exploitation of this data is at an all-time high. These growing dollar amounts have also caused more and more employee interaction with their plan. Typical employee plan interaction includes deciding where to invest these assets among an ever-growing menu of investment choices. All this participant activity is tracked and collected by the organization hired to handle the records of the retirement plan. This activity is tracked to provide employees ready access to information about their account and advise the employer as to whether retirement benefits are being properly utilized. Furthermore, tracking is necessary because the IRS requires that certain information about the plan be reported.

The employee, the employer, and the IRS are not the only people who have a keen interest in this information, however. Affiliated and third party marketing organizations are willing to pay dearly for access to valuable financial information about American workers.[6] As competitive forces continue to drive down the profitability of providing retirement plan administration services, the temptation for these service providers to use this data to augment existing sources of revenue is only going to increase. Under current law, however, a participant can do very little to stop the unauthorized use of their personal retirement plan data.

Developments in the Law of Personal Data Confidentiality

A century ago, a federal court in New York faced a privacy complaint that arose from the proliferation of a new technology. In 1902, it was a camera that caused Abigail Roberson to sue the Rochester Folding Box Company that year to halt the unauthorized use of her picture on a box of flour.[7] The court refused to halt the use of Abigail's picture for the purpose of selling flour on the grounds that an ordinary individual had no property interest in the use of her own likeness. The ruling proved quite controversial and did not stand for very long. Since that ruling, a significant number of laws have been written and legal theories developed to protect people from such a privacy violation.[8]

What cameras were to Abigail's era, the Internet and powerful computer servers are today. These devices are capable of storing, processing, and disseminating massive amounts of data very quickly, making it possible to invade individuals' privacy as never previously imagined. Despite all our legislative and common law progress in the area of personal privacy, current law gives the possessor of information substantial latitude to use, reproduce, or sell it, in whatever manner they see fit.[9] One reason

statutory protection for personal information is lacking is First Amendment[10] concerns for free flow of information. Put another way, "information, ideas, facts, and concepts—that vast array of human knowledge and expression—are not available to the public merely as a customary matter; their use is presumptively and powerfully protected by the Bill of Rights."[11]

A counter argument arises from the Fourth Amendment,[12] the U.S. Constitution's grant of a right to protection from unreasonable search and seizure. While the Constitution does not specifically protect the privacy of nonpublic personal information, the courts have provided some common law. In the landmark 1967 decision *Katz v. United States*,[13] the U.S. Supreme Court expanded on this notion of a Constitutional right to privacy when it held "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[14] This decision created a new threshold question for any invasion of privacy claim, whether there was a "reasonable expectation of privacy."[15] Undoubtedly, this question has important implications on the development of laws governing the protection of nonpublic personal financial information.

Much subsequent federal legislation placed limits on the Government. The Privacy Act of 1974[16] and the Computer Matching and Privacy Protection Act of 1988[17] were designed to prevent excessive data collection by the federal government and to prevent them from disclosing certain information without authorization. The Right to Financial Privacy Act of 1978 (RFP)[18] outlined new restrictions on the government's right to obtain nonpublic personal financial data from financial services organizations. Both the ruling in *Katz* and the subsequent federal privacy legislation dealt unambiguously with privacy protections for individuals.[19]

However, the law has historically considered retirement plan participants' personal data to be not the data of an individual, but that of the retirement plan. Because participants' individual plan records have historically been defined as that of an institution, this information has never been afforded the protection of the law.[20]

Not surprisingly, when Congress passed a recent attempt to protect personal financial information, Title V of The Financial Services Modernization Act (Gramm-Leach-Bliley Act or "GLB") of 1999,[21] it again omitted privacy protection for millions of retirement plan participants by assuming that all this sensitive data is the property of the retirement plan, not of the employees themselves.[22] This omission was somewhat understandable in 1978, when retirement-plan data was kept primarily on paper and aggregated for all participants. In 1999, however, when retirement plan data was increasingly kept as individual participant data, and generally stored electronically for immediate retrieval, such an omission suggests the possibility of a pro-business political compromise.

While Federal law may currently provide no privacy protection for retirement plan participants, there are other defenses against unreasonable invasions of privacy. Beginning with the 1890 law review article "The Right to Privacy" by Louis Brandies and Samuel Warren,[23] the common law right to privacy emerged as a powerful tool to protect individuals from unreasonable invasions of privacy. Invasion of privacy concerns were further developed by Dean William L. Prosser and then codified in the Restatement (Second) of Torts.[24] The Restatement specifically mentions income tax returns as the type of personal record that should not be available for public inspection,[25] implying potential liability for anyone who would divulge the type of information that is routinely available to retirement plan recordkeepers.

Other causes of action successfully utilized by individuals who feel the privacy of their personal information has been violated include: breach of contract, negligence, breach of confidentiality, fraud, right of publicity, trade secret misappropriation, trespass to chattels, conversion, and unjust enrichment.[26]

The crucial distinction, however, between the privacy tort Brandeis and Warren wrote about and the privacy invasion contemplated in this article, is here we are concerned with activity within retirement plans which are governed by ERISA. ERISA was primarily constructed to protect the rights of retirement plan participants by enacting rules that require disclosure, establish standards of conduct, and provide appropriate remedies and easy access to Federal courts.[27]

Congress' other goal for ERISA was to balance participants' interests against plan sponsors' need for regulatory relief from the myriad of complex and often conflicting local laws with which they were being asked to comply when they endeavored to offer

retirement plans to a group of employees residing in multiple jurisdictions. Congress accomplished this goal by making all matters pertaining to retirement plans a federal question.[28] ERISA's preemption rule is unusual and sometimes referred to as "super-preemption" because it preempts the states from taking action against retirement plans even regarding matters about which ERISA is silent.[29] This effectively strips plan participants of their ability to use state courts to remedy an invasion of privacy[30] and is particularly relevant today with over one hundred privacy bills pending in thirty-three states.[31]

Industry Practices Regarding Participant Data Privacy

With all the legal cards in the hands of retirement plan sponsors and the financial services institutions they hire to administer these plans, one would imagine that it must be open season on the personal financial information they possess. However, a limited survey of current industry practices and the current lack of public outcry for reform suggest otherwise.

Privacy watchdogs, such as the Federal Trade Commission (FTC), and most in private industry agree that the long-term goal of any regulatory scheme designed to oversee the privacy of online personal financial data is to maximize the full potential of the electronic marketplace.[32] Both parties understand that to fully accomplish this goal, consumer confidence in online privacy must be improved to increase consumers' willingness to participate in it. Not surprisingly, there is disagreement between regulators and private industry on how best to accomplish this goal.

In its latest report to Congress regarding Internet privacy, the FTC, citing its own recent survey and one conducted by Georgetown University Professor Mary Culnan, concluded that while there has been significant progress in the self-regulatory efforts of large consumer-orientated commercial Web sites, private industry efforts alone are still not sufficient.[33] These studies pointed to numerous examples of insufficient privacy disclosures and cases where the disclosures were misleading, as evidence that, left to its own devices, private industry is too interested in generating revenue to be objective about consumer privacy protection.

To rectify the situation, the FTC has recently changed its position. Previously, the FTC had called for more time to allow industry self-regulation efforts to catch up with its privacy protection recommendations. Apparently not satisfied with the progress of private industry, the FTC shifted its position in a recent report. It is now calling on Congress to pass legislation that, in conjunction with the ongoing self-regulatory efforts of industry, would require online companies that collect and store personal information to comply with the Commission's fair information practice directives. These directives require consumers be given the following: notice, choice, access, and security.[34] Title V of Gramm-Leach-Bliley is such a Congressional privacy initiative developed to protect personal financial information but, as already discussed, it does not apply to the data stored by employers in their retirement plans.

Survey of Recordkeeping Industry Privacy Practices

Because the FTC and Georgetown University surveys focused solely on consumer Web sites, and did not investigate the current self-imposed privacy protection practices of online retirement plan service providers, I conducted a limited survey of my own. In doing so, I contacted seven providers of online retirement plan services and asked to review their policies regarding the privacy protection and procedures for the data they maintain on millions of retirement plan participants. Using the four "fair information practices" set forth by the FTC as my evaluation criteria, I found no consistent industry practice for guaranteeing the privacy of retirement plan information.

All seven of the service agreements surveyed covered the security provisions these providers employ to protect participant data from falling into the hands of a party not expressly permitted to it. Five out of the seven surveyed gave some form of notice that addressed, even if incompletely, their information practices. Only one out of seven provided any language in its privacy policy about how a participant might access their information. They positioned it as a "Return of Information" provision. And finally, not one of the seven policies addressed participants' "choice" to opt-out of having their information used for secondary purposes or disclosed to an affiliate or third party.

I found it interesting that when asked, six out of seven of these firms were verbally adamant about their commitment to keep participants' information confidential, yet none of the providers surveyed

offered a written privacy guarantee in their service agreements. One provider was fairly explicit about its ability to disclose information to affiliated salesman, but here, like many of the other policies, the wording of the agreement was difficult to follow and would most likely be misconstrued by someone who did not know what to look for.

My limited survey of current industry practices suggests that service providers may be attempting to simultaneously achieve two conflicting goals; convince their customers that participant information is being kept confidential through obfuscated service agreement language, while leaving the door open to engage in information sharing activities with affiliates and third parties. In one service agreement, for example, the service provider put in italics for emphasis the statement, "*We do not disclose any nonpublic personal information about our current and former customers to anyone, except as permitted or required by law.*" Yet as I have already established, current law "permits" just about any kind of disclosure the possessor of institutional financial records might decide to engage in. This type of legal doubletalk needs to be exposed for what it is, meaningless at best, and misleading at worst.

Retirement recordkeeping services providers, like any private business, are driven by a profit motive. Within the past few years, many large financial services organizations such as Travelers Insurance, Coopers & Lybrand, United Asset Management, and most recently John Hancock Insurance have exited the business because they were unable to make money. Those that remain are investing increasing amounts in technology to stay competitive. Yet, they must deal with conflicting customer feedback about the best strategy to gain market share. On one hand, the public is clearly concerned about the confidentiality of their personal information,[35] making this an important business consideration. On the other hand, customers are looking for a low cost solution, and allowing for the secondary use of personal data can allow a service provider to meaningfully lower their price for retirement plan recordkeeping services.

Conclusion

Thanks to their increasing popularity and ten years of generally favorable investment returns, it is estimated that over thirty million Americans have accumulated nearly five trillion dollars in defined contribution plan assets.[36] The privacy risks to these assets are mounting. Because recent legislation purported to improve the confidentiality of personal financial data[37] leaves employees' retirement plan information largely unprotected, additional action is needed.

Even though retirement plan recordkeeping providers currently claim no intention to pursue profits from the sale of confidential participant information, similar pledges not to sell personal information "aren't worth the paper they're written on."[38] This leaves retirement plan participants wanting for some form of protection from the kind of unwanted privacy intrusions envisioned by the Founders and codified in the Fourth Amendment. Yet not at the cost of the viability of the organizations that provide the convenience of today's recordkeeping systems.

Some privacy scholars have advocated assigning property rights to personal financial information,[39] thus requiring service providers to contract individually for the secondary use of plan participants' personal financial data. The communication requirements of such a system, however, would be extensive and quite possibly render it unworkable in the context of retirement plan administration. Another approach would be to grant contact rights to the employer over its employees' personal financial data. This would greatly reduce administrative complexity and costs, as there now would be only one party for the service provider to negotiate with. On a case-by-case basis, and in advance, employers could be offered the opportunity to authorize the secondary use of participant information in exchange for a cost reduction for the participants.

An important factor in the viability of such a system is the employer's ability to negotiate. In other words, absent any regulations, there would have to be enough competitors remaining in the industry to provide employers with the leverage to negotiate such a contract on reasonable terms. The contract approach would also induce service providers to focus their efforts on creating new products and services that would have a high likelihood of being accepted by employers and therefore potentially reduce the unproductive use of participant's personal financial data. While this approach is far from perfect, because it still results in individuals' loss of control over their own personal data, and would undoubtedly cause conflicts between employer and employee, it would at least represent a step toward increased

control over confidential employee information at a viable cost.

It seems fair to speculate that the lack of national uproar over this issue is partially due to a concerted effort on the part of retirement plan service providers to limit the secondary use of this very valuable information. It is also likely that because there is less emotion attached to personal financial records than personal medical records, retirement plan privacy concerns have taken a back seat to the recently successful efforts to protect the information residing in employer health and welfare plans.[40] The recent implementation of federal rules protecting the confidentiality of employee medical records, combined with President Bush's campaign pledge to "guarantee the privacy of medical and sensitive financial records . . . [and] make it a criminal offense to sell a person's Social Security number without his or her express consent"[41] suggests that the timing might be right for privacy advocates to address the privacy of retirement plan participant data.

If the new medical records privacy rules are to be used as guidelines, retirement plan participants would receive the same types of privacy protections currently offered by GLB (notice, choice, access, security) along with an important enhancement. The recently released medical records privacy rules prohibit the unauthorized secondary use of employee data by anyone, including the possessor and their affiliates.[42] Regardless of the eventual outcome, it is safe to say that the current lack of privacy protection for retirement plan data needs to be brought out into the open so that the retirement plan sponsors can perform their fiduciary duty to protect the interests of plan participants.

Endnotes

1. JOHN H. LANGBEIN & BRUCE A. WOLK, PENSION AND EMPLOYEE BENEFIT LAW 6,6 (3d ed. 1999).

2. 29 U.S.C. § 1001.

3. 120 Cong. Rec. 29, 197 (1974) (statement of Rep. Dent noting that ERISA's "crowning achievement [is] the reservation to Federal authority [of] the sole power to regulate the field of retirement plans...eliminating the threat of conflicting and inconsistent State and local regulation.").

4. Mark Hoffman, *ERISA: Too much of a good thing?,* PENSION & INVESTMENTS MAGAZINE, Apr. 1999, at 14 (Washington-based Employee Benefit Research Institute estimates that while the number of pension plans has declined by more than 50% since 1974, the number of defined contribution plans has nearly quadrupled); *The Defined Contribution Market: Strategies and New Directions,* STRATEGIC INSIGHT OVERVIEW, Nov. 2000 (by the end of 1999, more than 30 million American workers participated in some type of employer-sponsored defined contribution benefit program).

5. Martin Fowler, *Average Value of 401(k) Plans Swell as Participation Continues to Grow,* DOW JONES NEWSWIRE, Aug. 29, 2000.

6. In 1994, the State of Florida offered to sell copies of its motor vehicle database for $33 million. Larry Rohter, *Florida Weighs Fees for Its Computer Data: Some See Profits; Others, Too High a Price,* N.Y. TIMES NAT'L., Mar. 31, 1994, at B9. (In 1998, NationsBank was fined $7 million for securities law violations of disclosing customer nonpublic financial information with its subsidiary affiliate, NationsSecurities. The affiliate convinced depositors to transfer assets from insured accounts to buy high-risk investments causing a number of senior citizens to lose a portion of their life savings). *Ex parte* AmSouth Bancorporation, 717 So.2d 357 (1998) (customer sues to recover from financial institution that used customer's nonpublic financial records to solicit unsuitable investments). In 1999, U.S. Bank settled a lawsuit claiming that it received approximately $4 million plus commissions (22% of revenue generated) for providing its customers' nonpublic financial information to a third party marketing organization, WALL ST. J., June 8, 1999, and press release from the office of Minnesota's Attorney General Mike Hatch, June 9, 1999.

7. Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902).

8. WIS. STAT. § 895.50(2)(b) (2000) (prohibits "the use, for advertising purposes or for purposes of trade, of the name, portrait of picture of any living person, without having first obtained the written consent of the person. . ."); RESTATEMENT (Second) OF TORTS § 652D (1977) (unreasonable publicity given to another's private life).

9. Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness,* 11 BERKELEY TECH. L.J. 1, 24 (1996) (noting that in a very few egregious cases, federal and state authorities will combine in an effort to halt widespread privacy abuses, e.g., a 1991 action

against TRW to halt the reporting of inaccurate financial records that damaged the credit rating of multiple individuals).

10. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press. . .").

11. Diane L. Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights,* 33 WM. & MARY L. REV. 665, 665 (1992).

12. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. . .").

13. Katz v. United States, 389 U.S. 347 (1967) (involving the Government's right to place a wiretap on a public phone).

14. *Id.* at 351-352.

15. *Id.* at 361.

16. Pub. L. No. 93-579, 88 Stat. 1897 (codified as 5 U.S.C. § 552a (1994)).

17. Pub. L. No. 100-503, 102 Stat. 2507 (codified as 5 U.S.C. § 522a (1994)).

18. 12 U.S.C. § 3401-13.

19. Spa Flying Serv., Inc. v. United States, 724 F.2d 95 (1984) (definition of "customer" limited to individuals and small partnerships of five or less).

20. Donavan v. Local 38, Plumbers & Pipe Trades Pension Fund, 569 F. Supp. 1488 (N.D. Cal. 1983) (citing RFA § 1115(a), RFA found not applicable to a subpoena directed to a bank that commanded production of retirement plan records).

21. 12 U.S.C. § 501-510.

22. *Id.* at § 504; Christopher H. Schmitt, *Think Your Secrets Are Safe?* BUS. WK., Apr. 9, 2001, at 88.

23. Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

24. Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet,* 34 SAN DIEGO L. REV. 1153, 1189 (1997) (citing William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960); RESTATEMENT (Second) OF TORTS § 652A-652I (1977)).

25. RESTATEMENT (Second) OF TORTS § 652D cmt. b (1997).

26. Gindin, *supra* note 24, at 1194-1195.

27. 29 U.S.C. § 1001(b).

28. Dukes v. U.S. HealthCare Inc., 57 F.3d 350, 355 (3d Cir. 1995) ("Section 514 of ERISA defines the scope of ERISA preemption, providing that ERISA supersedes any and all State laws insofar as they may now or hereafter relate to any employee benefit plan."); New York State Conference of Blue Cross & Blue Shield v. Travelers Ins. Co., 514 U.S. 645, 656-57 (1995) (summarizing intent of ERISA, "to ensure that plans . . . would be subject to a uniform body of benefits law; the goal was to minimize the administrative and financial burden of complying with conflicting directives among States or between States and the Federal Government. . .").

29. Daniel Fox & Daniel Schaffer, *Semi-Preemption in ERISA: Legislative Process and Health Process*, 7 AM. J. TAX POL'Y 47, 48-52 (1988).

30. *But see*, Dishman v. Unum, 2001 U.S. App. LEXIS 8529 (9th Cir. May 8, 2001) (health plan participant successfully sues for invasion of privacy in California for an "unreasonably intrusive" investigation); Holman v. Julius, 1997 WL 403641, at *4 (N.D. Ill. July 16, 1997) (plaintiff's claim that insurance company violated state statutes regarding mental health information does not rest on terms of her ERISA plan, thus, plaintiff's case is remanded to state court for lack of federal question jurisdiction).

31. Amy Borrus, *The Stage Seems Set For Net Privacy Rules This Year,* BUS. WK., Mar. 5, 2001, at 51.

32. Federal Trade Commission Report to Congress, *Privacy Online: Fair Information Practices in the Electronic Marketplace,* May, 2000 at iv.

33. *Id.* at 5, 7.

34. *Id.* at iii. ("Notice – Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it, how they use it, how they provide Choice, Access, and

Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site. **Choice** – Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided. Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities). **Access** – Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information. **Security** – Web sites would be required to take reasonable steps to protect the security of the information they collect from customers.").

35. *Id.* at 32 (citing a Gallup poll from the fall of 2000 of 573 Internet users which found that 82% were concerned about the privacy of their personal data on the Internet).

36. Fowler, *supra* note 5.

37. 12 U.S.C. § 501-510.

38. Heather Green, *Your Right to Privacy: Going . . . Going . . .*, BUS. WK., Apr. 23, 2001, at 48 (describing how numerous defunct Internet retailers with pledges not to sell customer data have done so in bankruptcy proceedings to raise cash to pay creditors, e.g., author cites Toysmart.com, Voter.com, Eve.com as recent examples of companies that have done so. EBay, while currently thriving, has also recently informed its customers of its right to sell customer data in an asset sale).

39. Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63 (1999).

40. Julie Appleby, *Health Privacy Rules Proceed But Protections May be Modified in the Next Year*, USA TODAY, Apr. 13, 2001, at 1B.

41. Jim VandeHei, *Bush Medical-Privacy Act is Part of Wider Strategy*, WALL ST. J., Apr. 13, 2001, at A12 (on the record comment Bush made to ZDNet, an Internet news service, shortly before becoming President).

42. Kelly Hagan, *HIPAA Patient Privacy Rules*, (Feb. 25, 2000), available at http://www.oahhs.org.