

**COMMENT TO THE
FEDERAL TRADE COMMISSION**

**GRAMM-LEACH-BLILEY ACT PRIVACY SAFEGUARDS RULE
16 CFR Part 3_-Comment**

Submitted by:

Professor Mark E. Budnitz
Georgia State University
College of Law

October 17, 2000

COMMENT

The Federal Trade Commission's Request for Comment asks a variety of questions in regard to the appropriate scope of the Safeguards Rule ("Rule"), the range of financial institutions to which the Rule should apply, the appropriate standards, and the degree of specificity which the Rule should contain. The Request asks whether the Rule should establish general standards or require particular minimum steps or minimum procedures.

Congress found that privacy and security were issues of major national importance. Otherwise it would not have taken the extraordinary step of enacting the exacting requirements contained in the Gramm-Leach-Bliley Act. Congress found that these were matters of great significance because the risk of invasions of privacy and breaches in security were substantial. In addition, surveys conducted over many years have consistently demonstrated that privacy is a major concern of consumers, especially when they use the Internet. Therefore, consumers may avoid using Internet-based financial services unless the law provides privacy protection. In order to effectuate Congress' objectives, the Rule should be broad in scope and establish specific minimum procedures.

In deciding how strong to make the Rule, the Commission should be influenced by evidence of the pervasiveness of privacy and security problems. Some may argue that Congress overestimated the extent of the problem. Others may contend that earlier problems brought to Congress' attention when passing the Act have been taken care of and will not reoccur. A popular industry response to fears of privacy invasions is to claim that consumers are at much greater risk every time they give their credit card to a waiter. That response ignores the far greater damage which can be done by a hacker breaking into a database and stealing tens of thousands of credit card numbers and other personal information. Hackers have used this information to make unauthorized purchases and to do far greater harm by stealing consumers' identities. Some have even posted this information on Web sites for all to share.

To assist the Commission in evaluating these positions, I have prepared a summary of privacy invasions and security breaches which were reported between January and September, 2000. These are included below as Attachment A.¹ The attachment does not purport to be comprehensive; without doubt there were many incidents which I have not identified. Indeed, it is well known that often companies do not publicize these occurrences.

¹ I have described past privacy and security problems in *Consumer Privacy in Electronic Commerce: As the Millennium Approached, Minnesota Attacked, Regulators Refrained, and Congress Compromised*, 14 Notre Dame Journal of Law, Ethics & Public Policy 821 (2000) and *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 South Carolina Law Review 847 (1998). Attachments A and B were prepared with the assistance of Anne-Marie Motto, a student at Georgia State University College of Law.

Another possible objection to a strong Rule may be that as consumers have become more accustomed to using the Internet, they no longer attach much importance to their privacy. Further, some may claim that Web sites are now far more respectful of privacy concerns. Attachment B provides significant recent evidence that this is not true.

Another reason justifying a strong, broad, and specific Rule is the fact, noted in the Request, that “the Commission does not conduct regular examination of financial institutions.” Absent the type of close and constant supervision to which other financial institutions are subject, the only hope for faithful compliance is the promulgation of a Rule which does as much as possible, within the boundaries set by the Act, to protect consumer privacy and ensure security.

The Request for Comment asks whether insuring the integrity of customer records and information requires granting consumer access to records. It has long been recognized and acknowledged that consumer access is the only way to effectively monitor the accuracy of information. Fair information practice principles developed by the Department of Health, Education and Welfare twenty-five years ago and adopted by government agencies in the United States, Canada and Europe include a right of access.² Our experience with the information maintained by credit reporting agencies proves that even with the access guaranteed by the Fair Credit Reporting Act, huge numbers of errors occur, and often are corrected only if the consumer brings a lawsuit.

For the reasons given above, I urge the Commission to issue regulations which are broad in scope, contain specific rules, and require particular minimum procedures.

² Federal Trade Commission, *Self Regulation and Privacy Online: A Report to Congress* 3 (1999).

ATTACHMENT A

PRIVACY INVASIONS AND SECURITY BREACHES REPORTED FROM JANUARY TO SEPTEMBER 2000

Dave Hirshman, *Buy.com suffers a privacy breach*, ATLANTA J. CONST., Oct. 17, 2000, at D3

As a result of a computer glitch, online shoppers were able to see the names and addresses of others using United Parcel Service's Web based merchandise return system.

Love Bug Variant Highlights Online Banking 'Vulnerability,' Sept. 27, 2000, Newswire, 2000 WL 7654094

Virus targets online customers of United Bank of Switzerland stealing information about customer bank accounts.

Sam Zuckerman, *Security Flaw Found at E-Trade. Internet Stock Brokerage Moves to Correct Problem*, Sept. 26, 2000 (visited Sept. 26, 2000) <<http://sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/09/26/BU22755.DTL>

An Internet security expert found a programming flaw in E-Trade Group's Internet operations. The expert claimed that due to a security mistake, customer data, including passwords, were included in E-Trade cookies and protected only with an easily broken type of code. Hackers could gain full access to customers' accounts, trade in the customers' names, and remove money from their accounts. E-Trade removed the account information from its cookies after the expert publicized his findings.

Shane Peterson, *Washington Closes Road to Drivers'-Info Abuses*, GOV'T TECH., Sept. 2000, at 44.

Washington's Department of licensing canceled a contract with The Insurance Information Exchange after an investigation indicated that the company was selling drivers' information. The company would provide home addresses and driving records, including violations and accidents, to anyone with a credit card and the driver's license number and date of birth of the person they wanted checked. State law allows disclosure of driver's records only for insurance underwriting and for employment purposes with a signed consent.

Pennsylvania has experienced similar problems.

Steve Gutterman, *Internet Hackers Hit Western Union Site*, ATLANTA J. CONST., Sept. 11, 2000, at A4.

Hackers made copies of the credit and debit information of 15,700 Western Union customers who had used the company's site to transfer money. The attack occurred when systems employees conducting regular maintenance on the site left parts of it unprotected.

FTC Wins \$37.5 Million Judgement From X-Rated Web Site Operators, FTC Press Release (Sept. 7, 2000) (visited Sept. 24, 2000) <<http://www.ftc.gov/opa/2000/09/netfill.htm>>.

Defendants purchased lists of nearly 3 million credit card numbers from a California bank. The Defendants, using at least five different merchant accounts, then used these numbers to bill consumers for web site services they never used. Over 90% of defendants' \$49 million yearly sales are alleged to have resulted from these unauthorized charges. The court awarded \$37 million in damages and barred the primary defendant for 10 years from owning, controlling, holding a managerial post, consulting for or serving as an officer in any business that handles consumer credit accounts.

Boy, 15, Who Crashed had Bought Car on Net, ATLANTA J. CONST., Sept. 10, 2000, at A6.

A 15-year-old boy bought a car over the Internet by using CheckFree to pay for the car with an electronic check. The check was drawn on the child support collection account of the Florida State Disbursement Unit.

TRUSTe Used 'Cookies' for Tracking, Group Says, ATLANTA J. CONST., Aug. 25, 2000, at F2.

TRUSTe, a group that issues "privacy seals of approval" to retail Websites, tracked its own users via use of cookies, a means not mentioned in its privacy policy.

Toys 'R' Us Suit Claims it Broke Confidentiality, ATLANTA J. CONST., Aug. 4, 2000, at F2.

Toysrus.com was accused of disclosing customer data to an outside marketing company, CoreMetrics. Both companies denied any wrongdoing.

eBay Agrees to Settle Privacy Lawsuit, ATLANTA J. CONST., July 28, 2000, at F2.

eBay sued ReverseAuction, accusing it of compiling eBay customers' email addresses and sending deceptive emails urging those customers to switch to ReverseAuction. ReverseAuction agreed to pay eBay \$1.2 million to settle eBay's lawsuit.

New York attorneys have filed a class action suit against AOL alleging that its Netscape browser captures and stores uniquely identifiable information when a person uses Netscape to download software.

Joris Evers, *Defunct Web Site Leaks Credit Card Info*, PCWorld.com, July 27, 2000 (visited Sept. 24, 2000) <<http://pcworld.com/pcwtoday/article/0,1510,17811,00.html>>.

All customer orders of a U.S.-based e-commerce site were openly available on line without any protection. The order information included customer names and addresses, credit card numbers and expiration dates, and items purchased (which were mainly pornography).

FTC Set to Challenge Toysmart.com to Prevent Sale of Consumer Data, ABI World, Headlines, July 10 - 12, 2000 (visited Sept. 24, 2000) <<http://abiworld.org/headlines/TODAY.html>>.

The FTC filed for a preliminary injunction against Toysmart.com, to prevent the company from selling the names, addresses and buying habits of its customers, despite the company's privacy policy guaranteeing that it would never share such information. Toysmart, which is majority-owned by Disney, had placed an advertisement in the *Wall Street Journal* to solicit bids for its customer lists and profiles. Disney offered to buy the lists and retire them, in order to ensure customer privacy. It is unknown whether any of the lists had already been sold.

FTC Announces Settlement with Bankrupt Website, Toysmart.com, regarding Alleged Privacy Policy Violations, FTC Press Release, July 21, 2000 (visited Sept. 24, 2000) <<http://www.ftc.gov/opa/2000/07/toysmart2.htm>>.

The FTC later agreed to settle the suit referred to above in exchange for Toysmart's guarantee that customer information would not be sold, except to a family-oriented Web site who is willing to purchase the entire package as a "qualified buyer" willing to abide by Toysmart's privacy policy. However, the FTC filed an amended complaint alleging that Toysmart violated the Children's Online Privacy Protection Act of 1998 by compiling names, email addresses and ages of children under 13 without obtaining parental consent.

Edmund Sanders, *Net Profiles May Curb Privacy*, ATLANTA J. CONST., June 28, 2000, at A8.

Many information brokers, including Experian and InfoUSA, sell lists of consumer names, addresses and phone numbers over the Internet. Lists of estimated income, buying habits, marital status and hobbies may also be purchased. These lists sell for as low as \$11.75, in sharp contrast to the costly and burdensome process of purchasing similar lists before the advent of Internet technology. Experian argues that it only sells lists of 50 or more names, and that no lists are released until the requestor provides a matching name and social security number and pays with a credit card. Experian also notes that the information contained in the lists is not obtained from credit reports, which may only be accessed by legitimate creditors. Rather, these marketing lists are generally compiled from government records, census data, real estate deeds, marketing surveys and warranty cards.

Information Brokers Settle FTC Charges, FTC Press Release, June 27, 2000 (visited Sept. 24, 2000) <<http://www.ftc.gov/opa/2000/06/touchtone.htm>>.

Touch Tone, accused of using deceptive methods to obtain private financial information about

consumers, agreed to settle a suit filed by the FTC. The settlement requires the information brokers to stop all unlawful “pretexting,” post a privacy policy on their Web site, and pay a \$200,000 suspended judgment if it’s determined that they misrepresented their finances.

I-Bonds, CDs: Amazing Rates, NEWSWEEK, June 26, 2000, at 64.

Missingmoney.com, a site which pools information from several unclaimed property offices, experienced a glitch which resulted in a woman’s personal financial data being flashed to anyone trying to log onto the site. The problem persisted for three days.

Maurice Tamman, *Danger Inside*, ATLANTA J. CONST., June 25, 2000, at P1.

Persons with high-speed Internet connections are especially vulnerable to hackers. A Georgia computer programmer was able to obtain a copy of all Internet traffic over his cable system, including Web pages, emails, log-ons and passwords - undetected.

Hackers Penetrate AOL Employee Files, ATLANTA J. CONST., June 18, 2000, at A10.

Hackers penetrated a small portion of AOL employee files in order to gain access to some personal user accounts, including credit card numbers.

Hope Viner Samborn, *Nibbling Away at Privacy*, ABA JOURNAL, June 2000, at 26.

Many plaintiffs have filed suit against RealNetworks, alleging that the company accessed its users’ hard drives to determine their music preferences.

Senator Robert Torricelli has proposed a bill that would prohibit companies from collecting information without the user’s permission.

Bank Customers’ Names, Addresses Not Protected by Constitutional Privacy Interest, 74 BANKING REP. (BNA), No. 21, at 939 (May 22, 2000).

The Pennsylvania Superior Court held that it was not unconstitutional for a bank to disclose the name and address of a customer to the police, without a warrant. The court held that disclosure of other information in bank and telephone records may be a privacy violation.

Fired Employee Sues Yahoo in Privacy Case, ATLANTA J. CONST., May 12, 2000, at H2.

A man sued Yahoo for disclosing his identity when he used a pseudonym to post disparaging remarks about his former employer on a Yahoo message board.

Anandashankar Mazumdar, *House Subcommittee Considers Legislation to Establish Privacy Protection Commission*, 74 BANKING REP. (BNA), No. 16, at 698 (April 17, 2000).

An information broker, who sold information about the Cosby family and impersonated Jon-Benet

Ramsey's father in order to get information to give to tabloids, is now serving time in prison for information theft.

Michael J. Sniffen, *British Hackers Charged With Credit Theft*, ATLANTA J. CONST., March 25, 2000, at B4.

Two 18-year-olds from Great Britain were charged with hacking e-commerce sites in five countries. The teens, using the screen name Curador, stole information from 26,000 credit card accounts and posted 6500 of the accounts on the Web. Computer experts say that a 2-year-old security hole in Microsoft's Internet Information Server software allowed the hackers to download the stolen information. Many small companies have failed to use the patch that was issued to correct this problem. The attack is estimated to have cost more than \$3 million.

Anandashankar Mazumdar, *Lawsuits, Bad Publicity Halt Company's Plan to Fully Exploit Net's Data Gathering Power*, 68 BANKING REP. (BNA), No. 35, at 2552 (March 21, 2000).

In the face of numerous privacy lawsuits, intensive government investigation, and public outrage, DoubleClick has agreed to hold off on plans to combine its anonymous Internet browsing data with the non-anonymous marketing database it purchased from Abacus Direct Corp until government and industry standards are solidified.

Steven Levy & Brad Stone, *Hunting the Hackers*, NEWSWEEK, Feb. 21, 2000, at 38.

On February 14, Yahoo experienced a denial of service attack (DOS), which is a deliberate attempt to shut down a network operation by overloading it with "huge tidal waves of data." This DOS attack caused Yahoo's server to slow, allowing only ten percent of its customers access to the site. The attack was traced to fifty different locations, indicating that the culprit was using someone else's machines to launch a calculated attack.

The next day, a series of similar attacks occurred. Buy.com's availability dropped to 9.4 percent. eBay was completely incapacitated for hours, and 95% of CNN.com's customers could not reach its home page. Amazon.com customers had to wait more than six minutes to connect to the home page.

On February 16, ZDNet.com and E*Trade's home pages were unaccessible for nearly two hours. Datek's site was inaccessible for 30 minutes, although they deny that this was caused by an attack. Access to Excite's home page dropped to 42.9 percent.

Jared Sandberg, *Holes in the Net*, NEWSWEEK, Feb. 21, 2000, at 46.

On February 16, hackers accessed the RealNames customer database, possibly stashing personal records and credit card numbers inside computers in China.

In 1996, hackers capitalized on software glitches to rewrite the CIA's home page to read "Central Stupidity Agency" and to include links to porn sites. A similar bug was used in 1998 to deface

the U.S. Army's website.

In January, a hacker exploited bugs in an on-line software retailer to lift 300,000 credit-card numbers. When the company refused his demand for \$100,000, he posted the customer's names, addresses and credit card numbers on the web.

In February, security analysts discovered that hackers were rewriting the price of items in "shopping cart" programs.

Gregory Vistica, *Inside the Secret Cyberwar*, NEWSWEEK, Feb. 21, 2000, at 48.

On January 24, 2000, the National Security Agency's extensive network of supercomputers mysteriously shut down for three days. Although the problem was later blamed on human error and a computer glitch, hackers have been attempting to access the NSA mainframe for years.

In 1997, hackers temporarily severed one of NASA's uplinks to the Atlantis shuttle. In addition, hackers have repeatedly disrupted 911 service in several states.

The Pentagon is particularly vulnerable to attack. Officials estimate that the Pentagon's computer system is hacked 250,000 times per year, 500 of which are considered serious. In fact, Russian hackers are known to have obtained some classified material from the Pentagon's system. And in 1997, hackers shut down the Pentagon's National Military Command Center, leaving only one fax machine working.

In 1998, teen hackers broke into the Air Force and Navy computer systems, and left trap doors so that they could regain access later.

Intelligence officials say that thirteen countries have programs directed at gaining access to U.S. computers.

Eileen Canning, *OCC Issues Alert Warning Banks to Keep an Eye on Security*, 74 BANKING REP. (BNA), No. 8, at 347 (Feb. 14, 2000).

Several popular internet sites, including E*Trade, Yahoo & eBay, experienced "distributed denial of service" attacks (DDoS). DDoS attacks involve security breaches which overload the sites with more information than they could handle, thus causing the sites to suspend service.

Ross Snel, *Hibernia and a Credit Union Sign Up With 'Screen Scraper'*, AM. BANKER, Feb. 8, 2000, at 1.

Yodlee.com, VerticalOne, Hibernia Corp. & First Tech Credit Union all engage in "screen scraping," the practice of allowing participating financial companies to provide their customers with information about accounts they have elsewhere. "Screen scraping" allows participating

companies to get customer permission to lift account data from the Web sites of other banks & companies, often without the knowledge of the company posting the information. Scrapers obtain customer's user names & passwords so they can log onto sites as if they were the customers themselves.

"Internet Privacy: An Oxymoron In Progress,?" PRIVACY TIMES, Feb. 3, 2000 (visited Sept. 29, 2000) <http://www.privacytimes.com/NewWebstories/oxymoron_priv_2_23.htm>.

Outpost.com, a site selling hi-tech gear, encountered a glitch that revealed customers' detailed transaction summaries, including e-mail, billing and shipping addresses, type of credit card they used, and their order history.

Due to a glitch in Microsoft Front Page, a software that allows subscribers to sign up online, the consumer information of 227 Florida customers has been exposed for two years. Credit card numbers, names, addresses, telephone numbers and passwords were displayed.

Many hackers are trying to exploit weaknesses in high-speed DSL Internet connections, with the purpose of taking over consumers' computers in order to launch anonymous attacks on others. Unfortunately, many DSL companies do not warn their customers of potential security problems, nor do they inform customers of the need to install firewalls to prevent these kinds of attacks. One user in England claims his firewall stopped seven electronic break-in attempts in three days.

John Markoff, *An Online Extortion Plot Results in Release of Credit Card Data*, N.Y. Times, Jan. 10, 2000, at 1.

A hacker stole more than 3000,000 credit card files from CD Universe, an Internet music seller. When the seller refused the hacker's demand for \$100,000, the hacker published 25,000 of the files on a Web site. The published information included credit card numbers, names, and addresses.

ATTACHMENT B SURVEYS OF CONSUMERS AND WEB SITES

Dose of Skepticism, ATLANTA J. CONST., Oct. 17, 2000, at D2

According to a Harris Interactive survey, 64% of online users believe e-businesses share personal information, and 59% believe businesses collect personal information without their knowledge. They were worried more about their personal privacy than about health care, crime, or taxes.

Derrick Cain, *Majority of Internet Users Disagree With Administration's Privacy Policy*, *Study Says*, 75 BANKING REP. (BNA), No. 8, at 284 (Aug. 28, 2000).

A report by the Pew Internet and American Life Project indicated that 86% of Internet users wanted an "opt-in" policy requiring e-companies to obtain users' permission before collecting and using personal information. The Clinton Administration, however, supports an "opt-out" policy, where Web sites have a right to track users unless users take affirmative steps to end the monitoring.

The study also revealed that 54% of users believe that web-tracking is harmful and an invasion of privacy. Only 27% of users considered tracking to be helpful in providing customer-tailored information.

Seven out of ten users would like more control over how e-companies track customer use. Of the 81% of users who want specific rules governing tracking, 50% felt that users should set the rules, 24% said the federal government should, and 18% said Internet companies should set their own guidelines.

Lucy Lazarony, *Online Privacy Policies Rarely Protect Web Visitors From Having Their Info Sold*, (visited May 22, 2000) <<http://www.bankrate.com/brm/news/ob/20000517.asp>>.

A study by Forrester Research indicated that 80% of Internet users want an online privacy policy that prohibits the sale of their personal information to anyone. 90% of users want some type of control over their information once it is released on the Web.

Only 8.5% of the top 1000 sites earned a four star rating. 30% had a privacy policy that allowed them to share customer data without permission and 37% of the top 1000 sites had no privacy policy at all.

Although the BBBOnline and TRUSTe award privacy seals to organizations which meet certain criteria, these seals are never revoked and are rarely enforced.

FTC Recommends Congressional Action to Protect Consumer Privacy Online, FTC Press Release (visited May 22, 2000) <<http://www.ftc.gov/opa/2000/05/privacy2K.htm>>.

The FTC concluded that while real progress has been made, it's not enough to "fully protect consumers' personal information and build public confidence in electronic commerce."

The FTC investigated numerous sites for compliance with four fair information practices: notice, choice, access, and security. The investigation revealed that only 20% of the sites randomly

sampled, and only 42% of the 100 most popular sites, had implemented all four practices. Even when only notice and choice were considered, 41% of the random sample and 60% of the popular sites provided acceptable disclosures.

Web Privacy Report: Yay, Boo, (visited Apr. 12, 2000)

<wysiwyg://9/http://www.wired.com/news/politics/0,1283,35594,00.html>.

A survey of 30,000 websites rated the sites' privacy policies from zero to four stars. Only 3.5% of the sites rated four stars. Four star sites never shared personal information with a third party, nor used the information to contact users without permission. 799 sites rated three stars, meaning that they would contact users and share personal information with third parties, but only with the user's explicit permission. 2580 sites earned the two star rating. Two star sites would contact users without permission, but wouldn't share information with third parties unless the user gave permission. 2251 sites earned a one star rating for sharing data without the user's permission. An astounding 22,000 sites were given a zero rating, meaning they had no privacy policy at all.

The study noted that most sites don't post privacy policies at all, and that even posted policies are changed often.
