Federal Trade Commission
Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information[1]
FTC File No. P034102
June 18, 2003

Beth Givens, Director
Privacy Rights Clearinghouse[2]

What's Missing from This Picture?

Note: These written comments are a longer version of the presentation given by Beth Givens at the FTC's "Information Flows" workshop on June 18, 2003.

Introduction

Thank you for the opportunity to participate in this panel on the costs and benefits of the collection and use of consumer information for customer relationship management (CRM) and targeted marketing.

The title of my presentation is "What's Missing from This Picture?" We have heard several industry representatives today touting the benefits of the collection and use of customer information. Industry themes include the benefits of convenience and cost-saving. In contrast, I want to focus on two themes:

- First, there are significant costs to individuals and to society of ***not*** protecting privacy.
- Second, not all costs can be expressed in monetary terms.

I would recommend that the FTC conduct additional research into both of these matters.

Background

The Privacy Rights Clearinghouse is a nonprofit consumer advocacy, research, and education program established in 1992 and based in San Diego, California. For 11 years, my staff and I have invited consumers' complaints and questions about a wide variety of informational privacy issues.

From the very first calls we received to our hotline in 1992, we have observed that control is a critical issue for consumers. The lack of control over what is done with their personal information is a big concern to individuals.

In the early days, the majority of our calls were complaints about unsolicited mail and telemarketing calls. By the mid-90s, identity theft became the number one topic on our hotline. Today, it's a mix of issues – telemarketing, identity theft, credit and financial issues, Internet privacy, and employment background checks.

People who contact us by phone and by e-mail explain how their personal information – in the hands of another person, a company, or a government agency – has in one way or another caused them harm, aggravation, or fear.

Public opinion polls show a consistently high desire by individuals to control the collection and use of their personal information. The following examples deal with information sharing by financial institutions.

- A 1998 AARP survey found that 81% opposed affiliate sharing without their consent.[3]
- A 2002 AARP survey in Vermont found that 89% say it is very important for financial companies to obtain permission before sharing data with other companies.[4]
- A 2003 California survey found that 85% would support an initiative requiring financial customers' consent before sharing personal information with other companies – and this result was obtained *after* the pollster read several arguments in favor of information-sharing, similar to the industry remarks concerning convenience and cost-savings made in today's workshop.[5]

Deceptive information-gathering strategies

I submit that a great deal of these strong feelings about privacy stem from the fact that deception and the lack of transparency form the foundation for the collection and use of a significant amount of consumer information.

Here is an example: One of the most deceptive information collection practices is the so-called product registration form, sometimes called the warranty card. These fold-over postcards are often packaged with consumer electronics products. In addition to asking the purchaser to indicate which product was purchased, typical forms also gather demographic information such as household income, ages of family members, education, hobbies, home ownership status, credit card usage, and the like.

But one's receipt is all that is needed to activate the warranty, and demographic data certainly has nothing to do with registering the product. Indeed, the deception goes further. The address that the postcard is mailed to is not the product manufacturer at all, but usually a post office box in Denver, that of the data aggregation company that compiles the data and sells it to marketers.

Yes, most such forms provide an opt-out statement. But it's written in vague language, in tiny print, at the bottom of the card. I have yet to meet an individual who has noticed it.

What is the result of the collection of consumer data via product registration cards? It's unsolicited mail and phone solicitations. Well, what's so bad about that? This is a question I often hear from industry representatives.

My reply is that many of the strategies used to market to consumers are based on deception, and are invisible to individuals. It leads to the perception, borne out in surveys, that individuals have no control over what is done with their personal information. And it contributes to the lack of trust that is reflected in numerous public opinion polls.

What the "free flow of information" really means

"The free flow of information." This phrase has a deceptively appealing ring to it, almost patriotic in tone. We have heard it used frequently by industry representatives during the workshop today. What are some of the consequences of the free flow of information?

Let's look at financial institutions as one example of what the "free flow of information" really means. Many financial companies have sold or shared their customers' names, addresses, phone numbers, account balances, account types, and account numbers (now encrypted) to telemarketing companies. Telemarketers in turn pitch products of dubious value to those bank and credit card customers – such as travel, entertainment, and shopping clubs, as well as insurance policies.

Several major U.S. financial companies have been sued by state attorneys general for their unfair and deceptive business practices involving the sharing and selling of their customers' personal data. These include U.S. Bankcorp, Citigroup, Chase, Fleet Mortgage, FirstUSA, and NationsBank.

What are some of the fraudulent and unethical practices involving the sharing of customer data?

- One practice is called pre-acquired account telemarketing fraud – where products and services are charged against individuals' accounts without their consent – achievable because the financial company shared the account number with the telemarketer. The Minnesota Attorney General sued U.S. Bankcorp for this practice.[6] Now banks and credit card companies are encrypting account numbers but the end result is still the same. Individuals' accounts can be debited without their knowledge.

- In the 2001 case *FTC v. Citigroup*, a former CitiFinancial employee explained in a sworn declaration that branch managers targeted deceptive loans to individuals who they identified as vulnerable because of being "uneducated, inarticulate, or a minority, or particularly old or young."[7]

- In an earlier case, NationsBank shared information about its customers' maturing CDs with its affiliated securities company, which in turn pitched high-risk investments to these individuals, many of whom were elderly. They were misled into believing that they were dealing with the bank and mistakenly thought the investments were safe. Many lost a good deal of their life savings.[8]

Costs to individuals of not protecting privacy

I mentioned in the introduction that I would talk about the costs to individuals and society of *not* protecting privacy. Certainly the fraudulent and unethical practices that I have just described have very real and significant costs to many individuals.

Telemarketer abuses

We are now witnessing the launch of the Federal Trade Commission's national do not call registry. It has been a long time in coming. I think it's fair to say that the strong political support for the registry is the result of the telemarketing industry's abusive use of personal information – even during a time when targeting has presumably been improving. By some estimates, telemarketers make over 100 million telemarketing calls per day. XX CITE

What are the costs to consumers?

- The expense of phone services such as unlisted numbers, Caller ID, Anonymous Call Rejection, Privacy Manager – of answering machines and voice mail services – of devices like the TeleZapper, the Phone Butler, and EZ-Hangup.
- The interruption of family time.
- The fear and aggravation caused by "abandoned calls," the result of the predictive dialing technology being set at too many outbound calls per hour.

Identity theft

I want to say just a few words about identity theft. Certainly, this crime is testament to the negative consequences of the "free flow of information." I want to focus on the tremendous cost to society of this crime. We often read estimates of the losses to banks, credit card companies, and merchants – and the out of pocket costs borne by the victims. But there are many more costs. One of the largest is the cost to the Internet economy – the fact that the major reason individuals do not shop on the Internet is fear of fraud and identity theft. XX CITE SURVEY PEW?

The negative consequences of collecting too much data

There can be negative consequences of collecting too much data:

- Does the health club need members' Social Security numbers? We've learned of several cases of members becoming identity theft victims because of dishonest employees' access to those numbers, including SSNs getting into the hands of terrorists. XX CITE NEWS ARTICLE

- A Michigan State University identity theft research project, soon to be published, is expected to announce that at least 50% of cases can be traced to employees of companies who have access to personal information on individuals. XX WEB

- Another negative consequence of collecting and retaining too much data is the cost of responding to subpoenas for the data that is on file – from enterprising divorce attorneys, to law enforcement investigations.

Stalking and domestic violence

I would be remiss if I did not mention the role of untrammeled information trafficking in the crimes of stalking and domestic violence. The National Network to End Domestic Violence, located here in Washington, D.C., is doing excellent work on these matters. (www.nnedv.org)

One becomes instantly sensitized, as I have, to the challenges of protecting informational privacy when attempting to assist individuals in keeping their residence address out of the hands of the batterer or stalker. You don't often think of one's address as being a highly sensitive piece of personal information, but to a victim of stalking or domestic violence, it is. The same holds true for individuals in certain occupations – law enforcement, court officials, school teachers, doctors, social workers, celebrities, political leaders, for example.

I encourage you who are designing CRM and targeted marketing systems to keep the needs of these individuals in mind. Let me give one example from my own experience with supermarket loyalty cards to illustrate how this can be done. I attempted to sign up for such a card with Ralph's supermarket by using the name "Ralph's Shopper" on the application form. I did not provide an address, and I fully accepted as a consequence that I would not be able to receive coupons through the mail. The manager at one Ralph's store refused to let me obtain a card because of my refusal to provide my true name and address. I went to another store and had no problem signing up as "Ralph's Shopper." I have successfully used my Ralph's card ever since.

What point am I making? CRM and targeted marketing systems should be designed to enable individuals who wish to remain anonymous to do so, while still enabling them to take advantage of at least some of the benefits.

The "miracle of instant credit"

Chairman Tim Muris in his opening comments today discussed "the miracle of instant credit." What is rarely discussed, however, is that the average household indebtedness in the U.S. is approximately $8,000. XX CITE When individuals become unemployed, many must file for bankruptcy because of their high credit debts. And they may lose their homes to foreclosure. The negative consequences to individuals and society of high household indebtedness are huge.

Let us not forget these negative costs when discussing the so-called "miracle of credit." In Fred Cates' morning presentation, he showed that lower-income persons receive a higher percent of credit cards -- and that this is beneficial to them. I would submit that many of these individuals are likely to be living off their credit cards with little hope of

ever paying them off. That is no miracle, especially when the interest rate is exorbitant. I would add that instant credit is a popular target of identity thieves who have *truly* discovered the miracle of instant credit.

Recommendations

What are my recommendations for remedying the situations I've described today? The collection, use, and sharing of customer data must be guided by the adoption of a robust set of Fair Information Practices – not just notice, or notice and choice – but also collection limitation, data quality, purpose specification, access, security, accountability, and enforcement. These are the Fair Information Principles developed by the Organization for Economic Cooperation and Development in 1980. XX URL The comments submitted by the Electronic Privacy Information Center (EPIC) discuss the Fair Information Principles in some detail. XX URL

Resources

In closing, I want to bring your attention to three papers that go into a great deal more depth on the issues I've just raised – the costs of not protecting privacy and the costs to society, both of which are often overlooked.

In preparing for this panel, I re-read the excellent paper by Robert Gellman, released March 2002, titled "Privacy, Consumers and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs Are Biased and Incomplete."[9] XX URL His paper has been contributed as an appendix to the comments prepared for this workshop by EPIC.

Second, I recommend that you read EPIC's comments as well. They offer a method for evaluating the costs of information flows. They analyze the quality of industry-sponsored studies. And they provide specific examples of how information flows have been used to increase prices, limit consumer choice, and to de-fraud consumers. XX URL

In reading both of these reports, I came to the conclusion that it would have been useful today to have individuals participate on these panels, perhaps economists, who can provide more insight into the larger societal costs of not protecting privacy. Professor Peter Swire's analysis in the final panel was excellent. There should have been more such contributions today. I will return to this observation in my closing remarks.

And third, you might be interested in comments I submitted to the Federal Trade Commission workshop on the "Information Marketplace" in March 2001, available on our web site.[10] XX URL In those comments, I provide a great deal more detail about the notion of deception as being at the root of a significant amount of information-gathering from consumers.

Closing remarks about the composition of the "Information Flows" panels

I am critical of the FTC for the industry bias in the composition of today's panels. The ratio of industry representatives to consumer advocates is nearly six-to-one (6:1). I counted 17 industry representatives, including the industry-funded think tanks. (Not counted in thais ratio are the two individuals from academic institutions, one of whom has been industry-funded, and one individual from the nonsectoral Ponemon Institute.) Only three consumer advocates made presentations during the day-long workshop – from the Consumer Federation of America, the publication Privacy Times, and from the Privacy Rights Clearinghouse. Hence, the 17:3 or a nearly 6:1 ratio of industry to consumer representatives.

During the final panel on "methodologies for identifying and measuring the costs and benefits for business and consumers," two industry-funded representatives were given the ability to make lengthy presentations without the opportunity for rebuttal by others -- Michael Staten of the Credit Research Center and Michael Turner of the Information Policy Institute. Both are from industry think tanks. In contrast, the earlier panelists were limited to about eight minutes each.

Further, Turner's presentation included allegations that the methodologies employed in consumer-oriented studies are faulty – namely, the recent Congressional testimony by Fordham Law School Professor Joel Reidenberg, and the writings of Evan Hendricks of Privacy Times. There was no attempt to enable those individuals or other consumer representatives to answer to those allegations.

In addition, the format for submitting questions to the panelists did not engender a "give-and-take" approach to discussion. Audience members were restricted to writing questions on cards and then handing them to the panel moderator. During the final presentation, when the two industry think tank representatives were literally given the floor, it was difficult to phrase a succinctly-worded question that would have been effective in questioning their allegations and supposed facts.

Instead, I would have preferred the ability to stand up and point out the shortcomings of *their* methodology – something that was difficult if not impossible to do on a 4-by-6 inch card. No doubt, others in the audience might have wanted the same opportunity.

I also would have appreciated the opportunity to correct some of the erroneous and misleading information presented about identity theft by Michael Turner during his presentation. But the format precluded my ability to do so. As one who has assisted victims of identity theft for a decade, either I or another identity theft expert should have had the opportunity to provide more balanced information on that topic.

The closing remarks on identity theft by Assistant Secretary Wayne Abernathy of the Treasury Department, while interesting and thought-provoking, also cried out for questions and discussion from members of the audience. Yet, questions were not allowed, not even on hand-written cards.

One of Secretary Abernathy's key points was that the solution to ending the epidemic of identity theft is for an *increase* in the flow of consumer information, not a decrease. If given the opportunity, I would have pointed out that the credit industry already has sufficient information to dramatically decrease the number of identity theft crimes committed, but that it does not use the information at its fingertips.

For example, credit grantors typically examine only the name, Social Security number, and credit score when making a decision on whether or not to grant credit to the applicant. This process is largely conducted in an automated manner, with no human interaction.

If credit issuers were to spend even a few more seconds per credit application, they would be able to note one or more anomalies when comparing the application to the named person's credit report – namely, a different address, a missing or erroneous date of birth, a different telephone number, a missing or erroneous mother's maiden name, and perhaps even misspellings in the applicant's name and address information.

Yet, the credit issuers do not use the very information that is available to them on credit applications and in credit reports. Secretary Abernathy's argument in favor of the "free flow of information" is not valid when discussing the solution to the crime of identity theft. Information is already flowing freely. It simply is not being used by the credit industry.

To conclude, the Federal Trade Commission, by its very mission of consumer protection, must be impeccable in presenting a well-balanced discussion of the issues in its workshops and other public policy forums. Deplorably, the "Information Flows" workshop, with its 6:1 ratio of industry to consumer representatives, did not present a balanced discussion of the "costs and benefits *to consumers and businesses* of the collection and use of consumer information" (emphasis added). I urge the Commissioners to strive in future workshops to discuss and debate the issues in a balanced and fair manner.

Thank you for the ability to participate in this workshop and to contribute these written comments.

---

[1] Federal Trade Commission, Public Workshop: Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information, 68 Fed. Reg. 20389 (Apr. 25, 2003).

[2] Privacy Rights Clearinghouse, 3100 – 5th Ave., Suite B, San Diego, CA 92103. Voice: (619) 298-3396. Email: bgivens@privacyrights.org. Web: www.privacyrights.org.

[3] "AARP Members' Concerns about Information Privacy," February 1999, report prepared by Kristin Moag, available at http://research.aarp.org/consume/dd39_privacy.html.

[4] "AARP Vermont Financial Privacy Survey," data collected by Woelfel Research, report prepared by Katherine Bridges, February 2002, available at http://www.research.aarp.org.

[5] "Findings of Statewide Survey on Financial Privacy Issues, data collected by Fingerhut Granados Opinion Research, February 2003, available at http://www.californiaprivacy.org and from Beth Givens. XX CITE

[6] Office of the Minnesota Attorney General, "Minnesota AG and U.S. Bancorp Settle Customer Privacy Suit," July 11, 1999, available at http://www.ag.state.mn.us/consumer/Privacy/PR/pr_usbank_07011999.html.

[7] *FTC v. Citigroup Inc.*, No. 1:01-CV-00606, Decl. of Gail Kubiniec, 10 (May 2001).

[8] *Nationssecurities and Nationsbank, N.A.*, SEC Release No. 33-7532, May 4, 1998, available at http://www.sec.gov/litigation/admin/337532.txt.

[9] Robert Gellman, "Privacy, Consumes, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete," March 2002, available at http://www.privacyrights.org XX.

[10] "The Information Marketplace: Merging and Exchanging Consumer Data," comments by Beth Givens, Privacy Rights Clearinghouse, submitted April 30, 2001, prepared for the Information Marketplace workshop of the Federal Trade Commission, held March 13, 2001, available at http://www.privacyrights.org XX and at the FTC web site, www.ftc.gov.