Privacy Self Regulation: A Decade of Disappointment

Chris Jay Hoofnagle

March 4, 2005
Dear Consumer,

To answer your question of what rights you have over the information that we have about you, there are none. We are a third party data collection company and we import information about each subject from several different sources including credit bureaus and utility companies. If you find that the information supplied to you from us is inaccurate, you may take that up with those companies.

Thank you for using LocatePlus.

Anne Ouellette
LocatePlus.com Customer Service

LocatePlus.com, Inc.
64 Central Street
Georgetown, MA 01833
978.352.6633
fax: 978.352.7799
www.locateplus.com

Front and Back Covers: Personal information available for sale, priced per thousand names. Inside Front Cover: Letter from Locateplus.com to concerned consumer forwarded to EPIC. Inside Back Cover: Lists sold of Magazine Subscribers.
Privacy Self Regulation: A Decade of Disappointment

Summary

The Federal Trade Commission (FTC) is capable of creating reasonable and effective privacy protections for American consumers. There is no better example of this than the Telemarketing Do-Not-Call Registry. The Registry, which was created and is now run by the FTC, makes it easy for individuals to opt-out of unwanted telemarketing. Now, more than 80 million numbers now no longer ring at the dinner hour.

Prior to the creation of the Registry, the telemarketing industry created self-regulatory protections that were largely useless. One had to write a letter to opt out of telemarketing, or pay to opt out by giving their credit card number to the Direct Marketing Association (DMA). The industry's self-regulatory efforts didn't even cover all telemarketers—only those that were members of the DMA. At its peak, the self-regulatory opt-out system had less than 5 million enrollments.

FTC's success in the telemarketing field demonstrates that it can protect Americans' privacy effectively and fairly. However, telemarketing was a 20th century problem. This report argues that it is time for the agency to move into the 21st century. It is time for the agency to apply the principles of telemarketing privacy regulation into the online world.

The FTC can protect privacy better than the industry can with self-regulation. We now have ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections.

New tracking technologies exist that individuals are unaware of, and old tracking technologies continue to be employed. Some companies deliberately obfuscate their practices so that consumers remain in the dark. Spyware has developed and flourished under self-regulation. Emerging technologies represent serious threats to privacy and are not addressed by self-regulation or law.

Self regulation has failed to produce easy to use anonymous payment mechanisms.

And finally, the worst identification and tracking policies from the online world are finding their way into the offline world. In other words, the lack of protection for privacy online not only has resulted in a more invasive web environment, but has also started to drag down the practices of ordinary, offline retailers.

EPIC calls upon the Federal Trade Commission and Congress to seriously reconsider its faith in self-regulatory privacy approaches. They have led to a decade of disappointment; one where Congress has been stalled and the public anesthetized, as privacy practices steadily worsened. We call on the government to create a floor of standards for protection of personal information based on Fair Information Practices.
I. The FTC Registry Is Better Than Market Alternatives

The Federal Trade Commission's (FTC) Telemarketing Do-Not-Call Registry was a stunning privacy success. Americans enrolled 10 million numbers in the Registry in its first day of operation. Now, the phone has stopped ringing on the more than 60 million numbers that were enrolled by the public. The nuisance of telemarketing will now be a thing of the past. Those who wish to receive telemarketing may still do so, but others have an easy option to preserve the dinner hour from interruption.

When one analyzes the decisions made by the FTC, it reveals that the agency took steps to effect consumers' desires. The FTC publicized the existence of the Registry and gave it a simple name and URL on the Internet. The FTC allowed people to enroll free by telephone or by the Internet. The FTC minimized "authentication" burdens. That is, the FTC made it easy for people to enroll by not requiring the consumer to jump through unnecessary hoops. Some from the industry suggested that only the line subscriber—not even a spouse or roommate—could enroll.

The Do-Not-Call Registry was a success because the FTC took the opposite approach from the self-regulatory system created by the Direct Marketing Association (DMA). In every respect, the FTC ensured that the Registry would be easy to use and fair, while the DMA's opt-out mechanism was difficult to use and relatively unknown.

The FTC's Registry is universal, free, and easy to use. Individuals could enroll online or by phone. The DMA's only applied to its members, cost money to enroll online, and was difficult to find. It's no wonder why the DMA's list only had 5 million enrollments, while the FTC's has more than 80 million.

These forces combined to make the DMA's market approach to telemarketing ineffective. The numbers speak for themselves. USA Today commented in 2002 that: "In 17 years, just 4.8 million consumers have signed up with the DMA's do-not-call list. By contrast, just five states -- New York, Kentucky, Indiana, Florida and Missouri -- have signed up roughly the same number in far less time."

Today's self-regulatory approaches to Internet privacy are much like the failed ones employed by the DMA for telemarketing. They are difficult to use, confusing, and often offer no real protection at all. This report details the current state of privacy on the Internet, and illustrates the myriad ways in which threats to privacy are becoming ever more grave, as new
technologies are developed, new practices become commonplace, and companies are not held accountable for disregarding privacy risks. Collection of personal information on the Internet runs rampant, both through direct and indirect means, both in the open and in secret. It is imperative that the FTC act now to correct these market failures. The FTC effectively and fairly corrected the failures of a 20th century nuisance—telemarketing. It is time for the agency to move into the 21st century and correct the failures of self-regulation to meaningfully protect Internet privacy.

II. Ten Years of Self-Regulation and Still No Privacy In Sight

EPIC has completed three Surfer Beware reports assessing the state of privacy on the Internet. "Surfer Beware I: Personal Privacy and the Internet," a 1997 report, reviewed privacy practices of 100 of the most frequently visited web sites on the Internet. It checked for collection of personal information, establishment of privacy policies, cookie usage, and anonymous browsing. The inquiry found that few sites had easily accessible privacy policies, and none of these policies met basic standards for privacy protection. However, at that time, most of the sites surveyed allowed users to access web content and services without disclosing any personal data. The report ended with a recommendation of continuing support for anonymity and the development of both good privacy policies and practices.

In 1998, EPIC produced "Surfer Beware II: Notice Is Not Enough," a report based on a survey of the privacy practices of 76 new members of the Direct Marketing Association ("DMA"), a proponent of self-regulation of privacy protection. The DMA released guidelines in 1997 that would require all future members of the DMA to publicize privacy policies and provide an opt-out capability for information sharing. Of the 76 new members surveyed, only 40 had web sites, and only 8 of these sites had policies satisfying the DMA's requirements. The report concluded that DMA's self-regulation efforts were not effective.

Fair Information Practices are commonly accepted responsibilities governing collection, access to, and control over personal information. They include:

- **Collection Limitation**: requires lawful, fair, and legitimate data collection.
- **Data Quality**: requires accuracy, completeness, and timeliness of data.
- **Purpose Specification**: requires entities to articulate why data is being requested and prohibits its use for other purposes.
- **Use Limitation**: requires consent for use of information inconsistent with the purpose of which it was collected.
- **Security Safeguards**: requires procedures to stop unauthorized access, use, modification, or disclosure of data.
- **Openness**: requires transparency of personal data practices, including notice of databases and the identity and location of the data controller.
- **Individual Participation**: requires access to, correction of, and sometimes destruction of personal information.
- **Accountability**: requires legal rights to ensure compliance.

The 1999 report "Surfer Beware III: Privacy Policies without Privacy Protection" assessed the privacy practices of the 100 most popular shopping web sites on the Internet. It examined whether these sites complied with common accepted privacy principles, used profile-based advertising, and employed cookies. The survey
determined that 18 of the sites had no privacy policy displayed, 35 of the sites used profile-based advertising, and 86 of the sites used cookies. None of the companies adequately addressed Fair Information Practices, commonly-accepted responsibilities covering collection, access to, and control over personal information. Surfer Beware III concluded that current practices of the online shopping industry provided little meaningful privacy protection for consumers.

The Federal Trade Commission ("FTC") has given self-regulation a decade to produce reasonable privacy protections online. The FTC first visited online privacy in 1995, and with minor fluctuations since then, has adopted a policy that embraces the idea that self-regulation is "the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology." It certainly is the least intrusive approach for companies exploiting personal information, but it has not efficiently ensured Fair Information Practices. Of the five Fair Information Practices endorsed by the FTC—notice, choice, access, security, and accountability—only notice can be said to be present as a result of privacy statements.

The first fluctuation in the FTC's commitment to self-regulation occurred in 1998, after the agency's survey of online practices showed that the lowest level of protection for consumer, notice of privacy practices, was not widely implemented. In a survey of 1400 web sites conducted by the Commission, 92% of the commercial sites collected personal information but only 14% had privacy notices. Of the commercial sites, only 2% had a "comprehensive" privacy policy. In reaction to these findings, the FTC was "still hopeful" that industry efforts would produce adequate privacy protections. At the time, Chairman Pitofsky recommended that Congress pass legislation if self-regulation failed to produce significant progress.

A year later in testimony to Congress, the FTC renewed its faith in self-regulation, noting that many web sites had adopted privacy policies. But protections beyond mere disclosure of practices lagged behind. Only a small number of surveyed sites had incorporated choice, access, and security into their practices. No meaningful avenue for enforcement existed at all. Commissioner Sheila Anthony concurred with the report's findings but dissented from its recommendations, noting, "industry progress has been far too slow since the Commission first began encouraging the adoption of voluntary fair information practices in 1996. Notice, while an essential first step, is not enough if the privacy practices themselves are toothless. I believe that the time may be right for federal legislation to establish at least baseline minimum standards."

In 2000, a 3-2 majority of the FTC formally recommended that Congress adopt legislation requiring commercial web sites and network advertising companies to comply with Fair Information Practices. However, a year later with the appointment of a new FTC Chairman, the FTC embraced self-regulation again. Chairman Muris decided to focus the Commission's attention on enforcing existing laws rather than create new legislative protections for online privacy. Chairman Muris indeed has expanded privacy protections through the creation of a do-not-call list and
with application of the agency’s powers to prevent unfair and deceptive trade practices.

The overall effect of the FTC's approach has been to delay the adoption of substantive legal protection for privacy. The adherence to self-regulatory approaches, such as the Network Advertising Initiative that legitimized third-party Internet tracking and the Individual References Service Group principles that concerned sale of SSNs, allowed businesses to continue using personal information while not providing any meaningful privacy protection. Ten years later, online collection of information is more pervasive, more invasive, and just as unaccountable as ever—and increasingly, the public is anesthetized to it.

It doesn't have to be this way. The FTC has been effective in protecting privacy when dealing with 20th century nuisances. It's time for the FTC to apply the lessons from telemarketing and other efforts to address the 21st century problem of Internet privacy.

III. Today's Tracking Methods Are More Pervasive and Invasive

Seven years ago, EPIC's report Surfer Beware I reviewed the status of Internet users' privacy rights and protections on the 100 most frequently visited web sites. The report was concerned primarily with the solicitation, collection, use, and protection of personal information obtained either from user-input forms or cookies.

Today, there are many more methods through which users can be tracked, profiled, and monitored in the online world. Cookie technology has matured—cookies are widespread and new uses have been developed. Entirely new technologies have emerged as well, some of which are all but unknown to consumers. Few of these methods are regulated, either internally by industry or externally by government. Without privacy legislation to protect Internet users from improper use of the information collected on the web, companies are unlikely to voluntarily cease privacy-invasive practices.

Cookies

Surfer Beware I discussed an Internet tracking technology over which there was "a great deal of controversy"—cookies. It found that about a quarter of the most frequently visited web sites used cookies. Today, many websites use cookies for one reason or another. In addition, there are several new wrinkles in the use of this tracking technology.

Third Party Cookies

Today, websites that a user explicitly visits are not the only entities which place cookies in your web browser—many web sites contain advertising served by outside commercial providers, and these providers may also send a cookie to your browser. These are known as "third party cookies." Some web browsers, such as Firefox allow users to block third party cookies.

Many web pages today have arrangements with third party ad servers that serve advertisements to their pages. For example, the MSN Privacy Statement lists two dozen third party ad networks that may place cookies in a user's browser.

Privacy policies (such as MSN's) tend to frame these third party cookies as a benefit to the user, allowing advertisers to "deliver targeted advertisements that they believe will be of most interest to you."

Persistent Cookies

A persistent cookie is one that remains on a user's computer after she has quit the browser. These cookies can be used to set and remember a user's web site preferences, settings, and passwords from one browser session to the next, but can also be used for
tracking and monitoring purposes. A troubling recent trend is to design these cookies to remain not just for many browser sessions, but for many years. Google's search cookie, for example, will not expire until January 17, 2038. This kind of long range tracking of users raises significant privacy risks.

**Web Bugs**

A web bug is a graphic on a web page that allows tracking and monitoring of visitors to that page. Web bugs are usually invisible, "clear" images only 1-by-1 pixel in size. They are capable of transmitting, back to the bug's originating server your Internet Protocol ("IP") address, the page you visited, the time you visited, browser information, and information from existing cookies in the browser.

---

**For market approaches to work, consumers must grasp both technology and practices. But in a Pew Internet Report, 56% surveyed couldn't identify a cookie.**

Web bugs are sometimes used for the innocuous purpose of counting how many times a particular page is viewed and gathering statistics about browser usage and web site usage. There are, however, much more invasive uses, such as compiling a detailed web-browsing profile of a particular user.

Web bugs are designed specifically to be secret and invisible. Many Internet users today are aware of cookies, and may perceive them from the appearance of visible advertisements. There are also tools to manage cookies. Web bugs, however, can transmit information and set cookies even when there is no telltale banner advertisement on the website tipping off a user that information might be collected about them. Furthermore, just one "allowed" cookie from an ad network opens the door for all web bugs within that network to collect browsing information about that user. With companies such as DoubleClick, providing advertising to countless web sites, this risk is significant. For instance, if a user with a DoubleClick cookie in their browser loads a web page with a DoubleClick web bug on it, that bug can grab the identifying information in the cookie and transmit it back to the server along with the other information collected by the bug.

**Google's Gmail Content Extraction**

On April 1, 2004, Google announced the launch of their new Gmail service. Gmail is a web-based e-mail service offering one-gigabyte of e-mail storage to users. Gmail is supported by advertisers who buy keywords, much like the Google search engine's AdWords advertising program, which lead to targeted advertisements displayed alongside an e-mail message in a Gmail user's inbox. Gmail uses "content extraction" (a term from Google's patents) on all e-mails sent to and from a Gmail account in order to target the advertising to the user.

---

"If Google ogles your e-mail, will Ashcroft be far behind?"
and personal information, but the content of private communications.

Spyware
Spyware and adware are extremely invasive and annoying technologies that have flourished in the self-regulatory world of Internet privacy. Both can be broadly described as pieces of software placed on a user's computer by a third party that perform unwanted functions. Spyware and adware collect information about the user, sometimes in complete secrecy without the knowledge of the user. Some programs display pop-up ads on the user's monitor, while others track and record everything the user does online. Information is sometimes collected by the programs for the sole purpose of sending that data back to an advertiser, and other times used to immediately serve pop-up ads to the user. Users often inadvertently download and install spyware and adware along with other desired computer programs, most commonly file-sharing applications. McAfee, an Internet security firm that sells popular virus protection and other personal computer security programs, reported more than 2.5 million "potentially unwanted programs" on its customers' computers, as of March 2004.

IV. More Invasive Tracking
Mechanisms Are on the Horizon
There are several new and emerging technologies that have the potential to present significant privacy problems as they become more advanced and more widely used.

Digital Rights Management
Digital Rights Management (DRM) systems use technical means to protect an owner's interest in software, music, text, film, artwork, etc. DRM can control file access (number of views, length of views), altering, sharing, copying, printing, and saving, through either the software or hardware of a computer or device.

"Digital copyright management systems...are not some remote, futuristic nightmare...they will enable an unprecedented degree of intrusion into and oversight of individual decisions about what to read, hear, and view."

Some DRM technologies are being developed with little regard for privacy protection. These systems require the user to reveal his or her identity in order to access protected content. Upon authentication of identity and valid rights to the content, the user can access the content. Widespread use of DRM systems could lead to an eradication of anonymous consumption of content.

DRM systems could lead to a standard practice where content owners require all purchasers of media to identify themselves. DRM can also link or tie certain content inextricably to one particular user. Windows Media Player, for example, has an embedded globally-unique identifier that can track users and the content they are viewing.

Trusted Computing
Trusted computing is a platform for pervasive DRM in personal computers. The Trusted Computing Group, an industry consortium with members Microsoft, Intel, Hewlett Packard, and Advanced Micro Devices, is overseeing the creation of industry-wide specifications for trusted computing hardware and software.

Trusted computing systems combine hardware and software elements to create a platform that gives software vendors an incredible amount of control over what users do with their computers. These systems have
been developed to protect the security of the computer from its owner when she uses proprietary or copyrighted information.

**Computer freedom itself is at stake here. DRM can convert a flexible, user-controlled computer into an inflexible, copyright-owner-controlled surveillance device. Your next computer may really be a TV that watches you.**

While trusted computing does enable a number of important security and privacy-enhancing functions, it also creates new threats to privacy and anonymity that should be seriously considered. For example, by augmenting the security functions already present on personal computers, trusted computing may offer greater protection from malicious programs or remote exploits. On the other hand, Trusted Computing could make it difficult or impossible for users to access content anonymously.

As trusted computing technology develops, it could have significant impact on computer users' privacy in the digital and online world.

**Single Sign On Services**

"Project Liberty" is an online identification and authentication system. It allows individuals to use a single sign-on in order to access many different web pages, and is being developed by a coalition of companies. A similar system has been designed by Microsoft, known as Passport or .NET Passport.

Identification and authentication systems present privacy risks for individuals. They can become virtual tollbooths for the Internet, requiring identity before one can view web pages. This violates a fundamental principle of privacy—the idea of collection limitation. It is illegitimate to collect information unless it is actually necessary to complete some function. However, with a proliferation of authentication systems, it becomes easier to compel individuals to identify themselves for no legitimate reason. These systems also enable profiling, which results in more spam, direct mail, and telemarketing for individuals.

**V. The Privacy Friendly Are Mimicking the Privacy Invasive**

In Surfer Beware I, EPIC noted that news web sites usually did not require disclosure of personal information in order to access their content, a practice that enhances privacy. The report stated that many of the top web sites allow "users to visit without giving up personal information. Anonymity plays a particularly important role for those sites...that are providing news and information to the on-line community." EPIC thought that it was especially appropriate for news sites not to attempt to identify site visitors, as anonymous access to political information shields individuals from law enforcement scrutiny and politically-motivated retribution.

But the ability to view the news anonymously is dramatically limited now. More and more news websites are requiring disclosure of personal information in various forms in order to access news articles.

EPIC conducted a survey of the websites of the top twenty-five US newspapers (by daily circulation). Thirteen of these top twenty-five sites require disclosure of some personal information in order to access content. Seven newspapers (including three of the top five) actually require "registration." All seven of these sites require disclosure of personally identifiable information. The other five sites require only disclosure of information which is not, on its own, personally identifiable (gender, postal code/country, and birth year).
Internet users are becoming increasingly frustrated with the prevalence of registration requirements on Internet sites. Evidence suggests that users will go out of their way to avoid divulging personal information on news sites. Many users who don't want to divulge personal information in order to read the news online are engaging in "privacy self defense," as they enter false information in registration pages, or turn to services such as Bugmenot.com. Bugmenot is a website through which users can "share" personal login information, and as of August, 2004, claims to have "liberated" more than 18,000 pages from the confines of required registration.

Online users have strong reservations about the use and abuse of their personal information. Surveys show that people value anonymity, especially on the Internet, and simply don't want to give up their information. A 2003 Annenberg Survey found that 57% of those polled believed that if a company has a privacy policy, the company will not share information with other entities.xv

The mere existence of a "privacy policy" also does not ensure that a person's information will remain "private" in the common sense of the word—both the LA Times and Chicago Tribune websites do not allow users to opt out of information sharing, advertising and communications from the newspapers and their "affiliates" (although you can opt out of sharing of your information with their advertisers and other third parties). There is also some indication that some newspapers have been checking the data provided at registration against third party commercial databases for accuracy.xvi

Compulsory site registration is likely to become a "vicious cycle" of privacy violations—increasing prevalence of privacy self-defense through providing "bad" or incorrect information might result in an increased tendency on the part of newspapers to require more invasive information from users, and to compare this information to commercial databases to ensure accuracy.

VI. Previous Self-Regulatory Initiatives Have Failed

Instead of driving towards legally accountable privacy frameworks, the FTC has a predilection towards self-regulatory initiatives. One notable effort was the NAI—The Network Advertising Initiative. The NAI was announced in 1999 shortly after DoubleClick, an online target advertising company, was the subject of a FTC investigation. The investigation was spawned by reports that the company was planning to link its anonymous surfing data with detailed offline customer profiles from Abacus Direct. Public protest led them to suspend their plans to merge their anonymous data with the personal information they had purchased.

Strong public opposition to online profiling caused Congress and the FTC to make efforts to address the practice. In November 1999, the FTC and Department of Commerce announced the formation of the NAI at a Workshop on Online Profiling. Less than a year later and with little involvement from consumer and privacy groups, the self-regulatory NAI principles were publicized.

The NAI standards were too weak to provide privacy commensurate with surfers’ expectations. They encompassed only notice, opt-out, and "reasonable" security. NAI members could transfer information amongst themselves to an unlimited degree, so long as
it is used for advertising. No meaningful enforcement mechanism was incorporated.

Even where the NAI set privacy standards, they were burdensome for individuals to exercise. For instance, users who didn't want to be tracked by DoubleClick's cookies had to download and leave an "opt-out cookie" in their browser. For those who think that deleting their cookies enhances their privacy protections, they will have to repeatedly remember to download the cookie.

Further contributing to the irrelevance of NAI is the fact that its membership has depleted to two: DoubleClick and Atlas DMT.

**New Tracking Methods Undermine the Already Weak NAI Provisions**

Behavioral targeting is becoming increasingly popular with web ads that follow users as they browse the web. These ads can be targeted to a visitor's online habits. Many of these ads rose in popularity from keyword searches, however, more omniscient tactics are also at work. Revenue Science, for instance, offers their customers web bugs to collect user information. Individual sites can determine which data gets used for targeting and the information collected does not get shared among different sites using the service. Customers of Revenue Science include ESPN, Reuters, Dow Jones, Newsweek, The Wall Street Journal and many others.

As more network advertisers benefited from electronic espionage, the relevancy of the NAI dwindled as the two member companies no longer controlled the industry. Companies such as Google, Overture, Aquantive and Omniture are all influential stakeholders in the targeted advertising market and profiling business. Although they are not NAI members, the common theme of self-regulation has remained popular. Not surprisingly, the core of the weak NAI principles can still be identified throughout the privacy policies of the major network advertisers.

**The NAI Principles Didn't Provide Privacy Then and Don't Provide it Now**

The NAI principles have not contributed to an environment where privacy is protected. Only notice has effectively been conveyed online. Although consent varies depending on opt-out/opt-in policies, most advertisers operate on a no consent or opt-out model. While access is often provided for, a user is often only given access to the information that they have voluntarily provided to the company. However, in order for meaningful access to be attained, a user must able to receive the same electronic profile that is of value to the marketer. Accountability and enforcement are equally meaningless concepts without a central authority to monitor and impose the standards. Without enforceable rights, Internet users will continue to be tracked and profiled as they become pawns of the advertising industry.

**IRSG: Freeing the Commercial Data Brokers From Privacy Responsibilities**

The Individual Reference Services Group (IRSG) Principles were developed by commercial data brokers in the late 1990s in order to manage fomenting criticism regarding their business model. These data brokers sold Social Security Numbers and detailed dossiers on Americans to marketers, insurers, private investigators, landlords, and law enforcement.

The IRSG Principles set forth a weak framework of protections. They allowed companies to sell non-public personal information "without restriction" to "qualified subscribers." The problem is that everyone with an account is "qualified."

Under the IRSG Principles, individuals can only opt-out of the sale of personal information to the "general public," but commercial data
brokers don't consider any of their customers to be members of the general public. For instance, data broker ChoicePoint gives individuals no right to opt out and claims that "We feel that removing information from these products would render them less useful for important business purposes, many of which ultimately benefit consumers."

The IRSG Principles have been carefully crafted in order to ensure maximum flexibility for data brokers. They represent another self-regulatory failure that has resulted in easy access to detailed dossiers on Americans by both commercial and law enforcement interests. By turning a blind eye to the commercial sector, Congress allowed commercial data brokers to become "Big Brother's Little Helpers." They have created a national data center of personal information for law enforcement.\textsuperscript{xvii}

**NAI and IRSG Were Successful—For Those Invading Privacy**

These self-regulatory initiatives served their purpose—to stop Congress from creating real, enforceable rights while allowing privacy-invasive activities to continue. They placated the FTC, causing Congress not to act. The end result has been that the FTC hasn't taken action to address traditional network advertisers or newer forms of privacy invasive tracking. Similarly, since Congress didn't act on data brokers, the IRSG has dissolved, and its member companies continue to sell personal information widely.

**VII. Anonymous Purchasing Options: Another Market Failure**

Even if a given online retailer extends strong privacy protections to customers, popular payment methods are not anonymous and provide an avenue for online profiling. Credit card companies use and sell personal information for target marketing, and provide an easy trail for law enforcement access to purchasing information.

Currently, there are not ubiquitous and easy to use anonymous online purchasing mechanisms. Companies in recent years have offered anonymous purchasing services based on various models, but these approaches tend to be cumbersome and costly.

In testimony to Congress in 1997, the Federal Trade Commission discussed anonymous payment systems and recommended that: "federal government should wait and see whether private industry solutions adequately respond to consumer concerns about privacy and billing dispute resolution issues that arise with the growth of electronic payment systems, and then step in to regulate only if those efforts -- be they market-created responses, voluntary self-regulation or technological fixes, or some combination of these -- are inadequate..."\textsuperscript{xviii}

How much longer does the consumer have to wait for user-friendly, ubiquitous anonymous payment options?

**VIII. Information [In]Security**

One of the five fair information practices endorsed by the FTC is security—the responsibility that data collectors take reasonable steps to assure that information collected from consumers is secure from unauthorized use.\textsuperscript{xix}

Collection of personal information creates security risks for individuals. As companies amass personal information or send it elsewhere for processing, the databases become attractive targets for malicious actors.

It is difficult for individuals to assess the security and integrity of data collectors' systems. And recent events indicate that security in the data collection and processing industries falls fall short of being "reasonable."
A recent case in point involves Acxiom, a publicly-traded corporation that sells personal data and processes it for client companies. In a written statement to the FTC in June 2003, Acxiom’s CEO assured that its security practices were "exceptional" and multi-leveled: "...it must be noted that Acxiom undertakes exceptional security measures to protect the information we maintain...and around the information we process for our clients to ensure that information will not be made available to any unauthorized person or business..."

A month after making this statement, Acxiom was informed by law enforcement officials that an Ohio man was able to download and crack Acxiom's password database. The method of stealing the personal information shows that Acxiom did have extraordinary security measures—the problem was that they were extraordinarily sloppy. The man, using FTP access operated for Acxiom's clients, was able to browse around Acxiom's system and download a single file containing all the passwords. In the course of the Ohio investigation, Acxiom learned that a second man used the same technique to access over 8 gigabytes of personal information from April 2002 to August 2003.

And, while the SSNs and credit card numbers of 20 million were accessed, the identities of companies that provided the personal information to Acxiom remain secret.

Acxiom did have extraordinary security measures—they were extraordinarily sloppy.

Other indications of information insecurity abound thanks to a California law that took effect in July 2003. That law requires data collectors to notify individuals when their data has been stolen. As a result, the public has heard of many information security breaches that normally would have been kept secret.

The first publicized notice of a security breach involved a banking consultant who had financial details on his computer. An office burglar stole the computer, which had credit line information, Social Security Numbers, and other bank account information. Since then, news of security breaches routinely appear in the national media.

IX. Bad Online Practices Are Leaching into the Offline World

The trend of collecting personal information and monitoring purchase habits is not strictly limited to the on-line environment. Increasingly, merchants are requiring consumers to produce identification or reveal personal information at the point of sale or when they wish to return or exchange an item.

What’s Your Phone Number?

Increasingly, cashiers are asking individuals for their phone numbers. This places individuals at risk that they will receive telemarketing based on the most trivial of purchases in the offline world.

Consumers don’t realize that giving a phone number to a cashier invites telemarketing under the "established business relationship" loophole to the Telemarketing Do-Not-Call Registry.

But the problem extends beyond a cashier's request for information, rather, it is the presumption that the disclosure of personal information has become a precondition of sale. While a customer may feel uneasy about revealing this information, many do not know that this disclosure is voluntary. And because
individuals want to shield their personal information from disclosure, some data companies have developed stealth information collection techniques for offline retailers. For instance, Trans Union, a credit reporting agency, offered "Translink / Reverse Append," a product that gave retailers name and address information from credit card numbers collected at the register. Consumers are not actually asked for their address, and probably are not aware that their address is discoverable.

The exact purpose for this information collection varies from store to store. Nine West asks for customer information in order to create a database of transaction histories for each customer, containing shoe size and width. Victoria’s Secret has recently begun asking customer’s for their telephone numbers so that they may be informed of promotions. Sometimes, it is difficult to find out how the information is being used.

**Grocers Get Loyalty and We Get Less**

Frequent shopper or loyalty card programs vary depending on the type of retailer or service. Generally, grocery stores will offer loyalty cards where a customer reveals a significant amount of personal information in exchange for a card which makes them eligible for in-store discounts. There is a high privacy risk associated with these cards as a great deal of personal data is revealed and all purchased are tracked.

Consumers are led to believe that they saving money when in reality, the prices at non-savings card stores are often lower.

A 2003 Wall Street Journal study found that "most likely, you are saving no money at all [from supermarket shopping cards]. In fact, if you are shopping at a store using a card, you may be spending more money than you would down the street at a grocery store that doesn't have a discount card."

The Wall Street Journal reported that, "...according to industry experts...[loyalty] cards are designed to make customers feel like they got a bargain, without actually lowering prices overall."

The Wall Street Journal study surveyed card and non-card grocery stores in five different American cities and concluded that "In all five of our comparisons, we wound up spending less money in a supermarket that doesn't offer a card, in one case 29% less. The author further wrote that "...according to industry experts, our shopping experience was typical, because cards are designed to make customers feel like they got a bargain, without actually lowering prices overall. 'For many customers, the amount of money saved has not risen,' says Margo Georgiadis, a specialist in loyalty programs at McKinsey & Co. The difference is that stores now make you carry a card to get the discounts, whereas before they just offered plain old sale prices."

**Making a Return? Your Papers Better Be in Order**

A review of the return policies of select retailers indicates that asking for identification for returns, even when an original receipt is present, is becoming a common practice. In some situations, this requirement is even printed on the receipt while other merchants fail to post any notice of this condition. While some retailers simply take the identification to match the name and contact information, others go as far as to enter the driver’s license number into their computer system. Often, a customer might not even know that this is
occurring, or they may feel as though the recording of their driver's license number is a necessary step. Given the sensitivity of the information contained on a driver's license, when combined with credit card information that is often available at a return, this practice places the customer at risk of identity theft.

**Consumer Returns Database**

Some point of sale return information is being added to a little-known system known as the "Consumer Returns Database." The database is offered by The Return Exchange which offers a standardized return system to retailers. It operates in real-time by monitoring consumer return patterns it helps merchants identify fraudulent or abusive customers.

It is unclear what standards are applied to identify an abusive customer, or the rights that a customer has to access and correct the database. A list of the retailers who participate in the database is not publicly available. By the time a customer is aware that negative information exists about them in the database, it is because they have already been branded as a fraudulent or abusive returner.

**Firing the Customer**

Combined, collection of returns information and loyalty behavior can tip the balance of power between the consumer and the retailer. Left unchecked, this data will be used for customer exclusion. As the Boston Globe recently put it, slow service or unattractive prices are being used "as a behavior modification tool to transform an unprofitable customer into either a profitable customer or a former customer."

There is a growing movement in the "customer relationship management" or profiling industry where businesses are encouraged to eliminate customers who complain or who return goods. Jim Dion, president of retail consulting firm Dionco Inc., recently urged storeowners to create disincentives for certain customers. Dion characterized 20% of the population as "bottom feeders," who complain and have low-levels of loyalty. Businesses, he argues, should try to eliminate these customers: "It'd be cheaper to stop them at the door and give them $10 not to come in." An article in DMNews quotes Dion as suggesting that retailers "should consider a preferred-customer database—prefer that they don't shop here."

"Filene's banned two sisters from all 21 of its stores last year after the clothing chain's corporate parent decided they had returned too many items and complained too often about service."

And major businesses are adopting these recommendations. Best Buy's consumer exclusion tactics were recently detailed by the Wall Street Journal. Literally, Best Buy is trying to eliminate its most savvy customers, ones that recognize good deals, in favor of less thrifty customers that the company can charge more. Other companies engage in consumer exclusion in more subtle ways, for instance, Harrah's casinos automatically identifies callers and charges them for hotel rooms based on their perceived profit potential. The company hides the profiling system because consumers, if fully informed, would find the practices creepy.

**First-Degree Price Discrimination**

"First-degree price discrimination," a practice where businesses attempt to "perfectly exploit the differences in price sensitivity between consumers," is a growing problem resulting from collection of consumer information. As Professor Janet Gertz has explained: "By profiling consumers, financial
institutions can predict an individual's demand and price point sensitivity and thus can alter the balance of power in their price and value negotiations with that individual. Statistics indicate that the power shift facilitated by predictive profiling has proven highly profitable for the financial services industry. However, there is little evidence that indicates that any of these profits or cost savings are being passed on to consumers. For this reason, and because most consumers have no practical ability to negotiate price terms for the exchange of their data, many characterize the commercial exploitation of consumer transaction data as a classic example of a market failure.\(^{xxxvii}\)

First-degree price discrimination is a goal of some in the information business. CIO Insight Magazine recently published an article discussing pricing ceilings where price discrimination is described as a goal for the industry: "The ideal strategy? To capture the value of the product or service for a particular customer or customer segment."\(^{xxxviii}\)

X. Recommendations

The FTC has to move into the 21st century and meaningfully address Internet privacy. Ten years of self-regulation has led to serious failures in this field. The online privacy situation is getting worse, so bad that offline retailers are emulating the worst Internet practices.

The FTC certainly is capable of protecting privacy online. It has to rise to the challenge and exercise more skepticism in the market as a proxy for consumer interest. Sometimes the market advances consumer interests, but when it comes to privacy, the market has been a driving force in eroding both practices and expectations. In order to rise to the challenge of effectively protecting individuals' privacy, we recommend the following:

- The FTC should abandon its faith in self-regulation. Self-regulatory systems have served to stall Congress while anesthetizing the public to increasingly invasive business practices. Self-regulation has only been reliable in promoting privacy notices, the least substantive aspect of privacy protection. The public's, and even the FTC's own conception of Fair Information Practices, commands a broader array of privacy protection including access, choice, security, and accountability.

- The FTC should reexamine the Network Advertising Initiative in light of the agreement's dwindling membership and the existence of new, more invasive tracking measures.

- The FTC should reexamine the IRSG Principles to ensure that they provide some measure of meaningful privacy.

- The FTC should investigate the emerging technologies identified in this report, including digital rights management, trusted computing, and single sign on services.

- The FTC should investigate the emerging offline business practices identified in this report, including unnecessary requests for information at point of sale or return, customer return databases, customer exclusion, and first degree price discrimination.

- The FTC should work with the banking agencies to develop a unified mechanism for opting out under the Gramm-Leach-Bliley and Fair Credit Reporting Acts. Just as it made no sense for individuals to opt-out of every telemarketing call, it currently makes no sense for an individual to have to contact every single financial institution separately to protect privacy.
*This report was written with assistance from EPIC Internet Public Interest Opportunity Program (IPIOP) Clerks Dina Mashayekhi, Tara Wheatland, and Amanda Reid.


n505124.shtml.


ix Ad4Ever; AdCentric Online; Ad Dynamix; AdSolution; Avenue A; BlueStreak; BridgeTrack; DoubleClick; efluxa; Enliven; Flycast; 133; Mediaplex; PlanetActive; Pointroll; Profero; Qksrv; RealMedia; RedAgency; TangoZebra; TargetGraph; TrackStar; Travelworm; Unicast.


xv Joseph Turow, Americans and Online Privacy: The System is Broken, Annenberg Public Policy Center, June 2003.


xxii Customer Data Was on Stolen PC, Wells Fargo Says, Reuters, Nov. 21, 2003.


xxvi Id.

xxvii Id.

xxviii http://www.thereturnexchange.com/


xli Id.

xlii Id.


xliii Gary McWilliams, Analyzing Customers, WALL STREET JOURNAL, Nov. 8, 2004.


xlv Anthony Dann & Oscar H. Gandy, Jr., All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining, 40 JOURNAL OF BUSINESS ETHICS 373, 381 (2002).


xlix Id.
Maxim
Published by Dennis Publishing, Maxim is the essential guidebook for young men.

Key Segments

1,743,000 Universe / Base Rate $105.00 /M
1,327,000 Total Male Subs + $8.00 /M
129,000 Total Female Subs + $8.00 /M
600,000 6 Month Subs + $6.00 /M
314,000 3 Month Subs + $11.00 /M
117,000 1 Month Subs + $16.00 /M
128,000 Change of Address + $11.00 /M
36,000 Canadian + $21.00 /M
Catalog Rate $85.00 /M
Fundraiser Rate $75.00 /M

LIST TYPE
Consumer

SOURCE
Direct mail sold

GEOGRAPHY
Domestic (US) and Canada

LIST OWNER
Dennis Publishing

LIST MAINTENANCE
New to ALC 12/01/2002
Counts through 06/30/2004
Last update 07/13/2004
Update frequency MONTHLY

UNIT OF SALE INFORMATION
Average: $17.94

GENDER PROFILE
Male: 77%
Female: 7%

INCOME
Average: $5,000.00

SELECTION CHARGES
1 MONTH HOTLINE $16.00 /M
3 MONTH HOTLINE $11.00 /M
6 MONTH HOTLINE $6.00 /M
BUSINESS ADDRESS $11.00 /M
CHANGE OF ADDRESS $11.00 /M
GENDER/SEX $8.00 /M
KEYING $3.50 /M
PAID $8.00 /M
SCF $8.00 /M
SOURCE $8.00 /M
STATE $8.00 /M
ZIP $8.00 /M

ADDRESSING
CATALOG $45.00 /M

NEWSWEEK CATHOLIC SUBSCRIBERS

416,634 Catholic Subscribers $95/M
Counts are through June 2004

DESCRIPTION:
NewswEEK has identified the Catholic subscribers with InfoBase lifestyle and demographic information. NewswEEK Catholic subscribers not only respond to Catholic appeals but to a variety of other fundraising and non-profit organizations dedicated to humanitarian, cultural and health causes.

HEARST MAGAZINES INTERNET SUBS AT POSTAL ADD

366,792 Active Subscribers $130/M
83,348 3 Month Hotline Subscribers ADD $15/M
Counts are through June 2004.

DESCRIPTION:
These consumers have visited the Hearst Magazine's websites and subscribed to one of their magazines via the internet. These names are available on a one-time use basis and are at home addresses.


Reader's Digest provides an enriching breadth of editorial that meets subscribers' insatiable appetite for service journalism, current events, humor, and adventure that stem from The Digest's core affinities-health, home, family, finance, and faith.