The Ethics of Internet Privacy

Andrew S. Chiu

April 7, 2000

"Effective advertising is the key to keeping the Internet free, and personalized ads allow consumers to see information about goods and services that are relevant to their lives."

-Josh Isay, Director of Public Policy at DoubleClick, Inc

Introduction

An individual's right to privacy has always been highly cherished in the United States. This is in part due to the fact that the consequences for victims of privacy intrusions can be disastrous, ranging from hurtful rumors to identity theft and even ruined credit ratings. While most invasions of privacy are discreet, of little material value, and ostensibly do little harm beyond additional "junk mail," such indiscretions already worry the minds of Americans everywhere. The advent of the Internet and a tracking technology called "cookies" brought about a myriad of helpful tools and resources, from virtual stores to online medical libraries, as well as a host of privacy issues that remain as yet unresolved.

Although the Internet has achieved popularity with most of the general public, many remain unfamiliar and skeptical about the level of security and privacy on the Internet. According to a recent Business Week/Harris poll, 82% of those surveyed expressed substantial discomfort with “user profiling,” a practice in which companies track and record users' online movements. Much of this anxiety is attributable to the fact that users have no clear understanding regarding the rules that govern this practice, how extensive it is, what is recorded, and even how the information is used. Their apprehension manifested itself recently in overwhelming public indignation over prominent Internet advertiser DoubleClick, Inc.'s decision to link its millions of anonymous Internet user profiles with more specific information such as names and addresses of over 90% of U.S. households. By linking their profiles with direct-marketing databases, DoubleClick sought to gain much more detailed information about Internet users and their preferences. Unfortunately, DoubleClick has not been the only company to come under fire recently for its user profiling methodology and privacy standards. The list of companies includes Internet companies RealNetworks and Amazon.Com, and even household names such as Chase Manhattan Bank and Sony.

The DoubleCIick example is only one in a recent rash of publicized Internet privacy issues, all over business uses of customer information and user profiles. While swapping customer profiles, mailing lists, and other demographical information has long been standard practice, the combination of Internet technology and traditional databases brings to light some subtle business-ethics issues in the realm of consumer privacy. In particular, the very practice of user profiling is incongruous with the expectations of users who expose some personal details on a web site. Research done by the Electronic Privacy Information Center demonstrates the typical expectation of users is that their information will not be shared with advertisers who build profiles for the purposes of sending advertising.

In examining the business and ethical issues regarding Internet privacy, this paper will address the following questions:

1. What business and ethical issues are presented in the sale or use of Internet user profiles in conjunction with current household and/or confidential information?

2. How is the collection and dissemination of user profile and household information governed? Are there any gaps in the law that could work to the detriment of consumers?

3. What propositions are under consideration or have been enacted to protect consumers? Do additional protections need to be in place?

A Brief History of User Profiling

To properly examine the ethical issues surrounding the practice of user profiling, one must first look at the rationale behind such a practice to begin with. While an in-depth look at the technology that drives user profiling is beyond the scope of this paper, a brief history will suffice to readers up-to-date on the justifications for such a system.

During the infancy of the Internet, businesses seeking ways to develop an additional distribution channel ran into an unexpected technological challenge. The World Wide Web, originally designed as a publishing engine for academics, lacked the capacity to distinguish between different users and their requests for information. While this feature was wholly unnecessary the Web's initial purpose, its absence stymied attempts to implement transaction management--a key part of electronic commerce. Without the ability to remember each user as a distinct entity, web servers had no way of knowing who was in what stage of the purchase process. To facilitate the growth of e-commerce, Netscape Communications, Inc developed the first “cookies,” small files capable of temporarily storing small amounts of information on a user's hard drive.

Originally designed for transaction management purposes, companies quickly realized that cookies had other uses as well. Cookies could store information that could be used to help businesses personalize a user's web-experience and thus offer greater perceived value to a customer. Companies began using cookies to store everything from personal information to browsing and purchasing patterns. As companies expanded their use of cookies, their personalization capabilities increased to the point that they could even tailor content to a user's predicted tastes, and offer specific services such as reminders and special notices. To take advantage of these personalization features, users are required to “register” with a site, providing contact information, and other personal facts.

With companies seeking ever more information about consumers in order to provide better service and products, some have begun tapping into the wealth of consumer information on the Internet. However, most efforts have been limited to anonymous online profiling of consumers, without linking the data to real-world household databases. Internet advertising is still largely not understood, unfortunately defying many of the known rules and guidelines to successful advertising. As a result, online marketers are having difficulty providing completely detailed information on market demographics to their clients. With the prospect of losing substantial online advertising business in the near future, many online marketers have turned to combining user profiles with direct-marketing databases, in an effort to learn even more about consumers.

Internet Privacy

Today, the practice of user profiling is standard for most popular web sites. Users are required to provide numerous personal facts, from full name and contact information to hobbies and personal interests. As users browse the World Wide Web and sign up for various web sites, the personal information they leave acts similarly to a digital fingerprint. While this can be useful information in evaluating users and providing higher levels of service, most users do not know their digital "fingerprints" are highly prized by many other companies seeking to tap into the wealth of consumer information on the Internet. Most users, when divulging personal information to a web site, also never realize that their information is in fact being shared with online marketers.

Privacy violations on the Internet are not limited only to web sites exchanging lists of user profiles. Unsuspecting users posting personal information have had their credit card numbers and other important personal data stolen in classic cases of identity theft. Even more shocking is a recent Georgetown University survey of 21 health-care sites, in which several were noted for sharing users' names, ages, and even the email addresses.

The implications of such improprieties with modern user profiling techniques are enormous. The combination of user profiles accurate enough to correctly identify individuals, as well as highly accurate household databases containing address, medical, racial, or religious, indicates that it would be possible to determine which households visit certain sites. This practice seems harmless at first glance, and quite analogous to current targeted advertising techniques in which advertisers design different advertisements and air them at specific times to reach specific audiences. However, the same databases could be misused without individuals ever knowing how or why their lives were affected. Consider the following scenarios:

Scenario 1: Employers query databases and online profiles to determine the browsing habits of applicants, in order to ascertain their predilection towards certain "deviant" tendencies.

Scenario 2: Banks incorporate into their loan approval process a check against a data warehouse and online profiles to determine whether a "high risk" applicant frequently plays online sweepstakes and lotteries. Unbeknownst to the applicant, this information is used to assess the applicant's risk and credit-worthiness.

Scenario 3: Health insurance companies examine traditional direct-marketing databases and user profiles to see if applicants have been looking at cancer pages. Those applicants are then quoted higher premiums, in an effort to lower the number of potential cancer patients covered by the company.

These are only three possible scenarios, but they illustrate an important point -that users may never know how their information is used, nor even its potential impact upon their lives. This possibility is unfortunately the reality, since few users have any knowledge of how their information is used, whom it is sold to, and how those third parties choose use it. In addition, another danger exists due to the limitations of the technology. Consider the following situation:

Mike sits down and logs into Yahoo Inc.'s auction section, in hopes of finding that new Palm Pilot he's been wanting. Moments later his friend Dave walks over and asks to borrow the computer for a minute, to check on status of another auction. Mike agrees and goes to get a soda from the vending machine. Dave, unbeknownst to Mike, instead visits Yahoo's "Adults Only" chat rooms, spending several minutes there and engaging in a brief discussion. A week later Mike begins to

receive phone and email solicitations from companies selling "adult" merchandise and wonders why.

In the above situation, Yahoo was following standard practice and tracking Mike's browsing habits. It dutifully recorded Mike's entry into the "Adults Only" chat rooms, and noted the duration Mike supposedly spent there. If Yahoo sold that data to an online marketer who was then approached by an adult merchandiser, individuals such as Mike could be mistakenly handed over in a list of those users interested in adult topics. This lack of control worries many Internet users, especially those without the background knowledge to understand the underlying technologies. The Business Week/Harris Poll results show that an overwhelming 97% of those polled are uncomfortable with the prospect of user profiling with links to real-world personal information.

However, there are nevertheless compelling business reasons to profile users and exchange data.

Profiling does help many web sites provide better service, since they can use some of the information to enhance a user's experience. For example, once a user registers at Amazon.com, the site tracks the types of books viewed and purchased. As time passes, Amazon.com learns what a particular customer enjoys and promotes those types of products historically more relevant to a particular user. By exchanging user databases with another site, Amazon.com might also be able to learn more about what kinds of people like certain books, and tailor its service that way as well. In the realm of the Internet, where barriers to entry are relatively low and dot-coms are a dime-a-dozen, marginal increases in customer service or intrinsic switching costs can mean the difference between success and failure.

Current Governance[1]

Current privacy laws do little to protect users from zealous online marketers. Most online marketers or web businesses claim that usage of their web sites is entirely voluntary, although they do admit that usage is contingent upon registering and thus divulging at least a little private information. While there are few laws protecting adults online, the Federal Trade Commission (FTC) enacted the Children's Online Privacy Protection Act of 1998, designed to protect the rights of children online. Its provisions, set to go in effect on April 21, 2000, stipulate that webs site operators must:

1. Post the privacy policy. Web sites directed at children or that knowingly collect information from children under the age of 13 must post a notice of their information collection practices that includes:
    a. types of personal information collected from children,
    b. intended use of the information,
    c. information dissemination plans, and the involved third parties,
    d. a specific contact at the site.

2. Get Parental consent. In most cases, a site must obtain parental consent before collecting, using, or disclosing personal information about a child. Exceptions for email addresses are only for:
    a. response to a one-time request from a child,
    b. providing notice to the parent,
    c. ensuring the safety of the child or site,

[1] Legislation summaries may not contain the exact phrasing as set forth in the bill.

d. sending a newsletter or other information on a regular basis, as long as the parent is given notification and ratifies the agreement.

The penalty for violating the Children's Online Privacy Protection Act is $11,000 per infraction.

These provisions are an excellent beginning for online privacy laws, and are expected to allay the fears of many parents, who are wary of their child's privacy while on the Internet. However, this law does nothing to increase protection for the rights of adults. Fortunately, due to the overwhelming public attention given to online privacy as a result of violations by several well-known firms, approximately 20 states and the U.S. Senate are in the process of enacting bills to protect everyone's online rights. These states include New York, Hawaii, California, Maryland, and Virginia.

Of note are the efforts of U.S. Senators Ron Wyden (D-Ore), Conrad Burns (R-Mt), Robert Torricelli (D- NJ), and Russell Feingold (D-Wi). These four Senators have sponsored legislation, now in debate by certain committees, for the purpose of creating new or modifying current laws protecting privacy in general.

The proposed Online Privacy Protection act of 1999 (1999 5.809), sponsored by Sen. Wyden and Sen. Burns, would in essence extend the protections granted children in the Children's Online Privacy Act to all persons. Most importantly, it would require website operators to:

1. Provide a clear and conspicuous notice on the site regarding:
   a. The operator's identity,
   b. Any personal information collected,
   c. How the personal information is used by web site, and
   d. What information is shared with other companies.

2. Provide a meaningful and simple online process for individuals to consent to or limit disclosure of personal information for purposes unrelated to those under which the information was obtained.

3. Upon request of a person who provided personal information to the website or online service:
   a. Provide a description of the specific types of personal information collected which was sold or transferred to an external company,
   b. Provide a reasonable means for the individual to obtain the personal information from the external company, and
   c. Establish and maintain reasonable measures to protect confidentiality, security, and integrity of any personal information collected or maintained.

The most significant portions of this proposed legislation are those corresponding to the above parts 2 and 3. Part #1 is intended as a disclosure clause, to force web sites to more prominently display their privacy policies and explicitly describe their profiling practices. Important, nonetheless, for the public which expressed confusion as to the exact privacy policies of most sites.

Part #2 requires web sites to provide either of what is commonly known as an “opt-in” or “opt-out” capabilities. This clause would return some measure of control over personal information back to the user. Current profiling practices are typically “opt-out,” indicating that users must explicitly notify the site not to sell or exchange their data. “Opt-in” is a stronger form of control because it requires that users explicitly notify a site when they would prefer the exchange or sale of their

personal information. Online marketers have protested vehemently that enforcing "opt-in" policies would in effect extinguish the derived online marketing benefits of user profiling. Users, they claim, would not go through the trouble to permit their information to be used. However, privacy advocates insist that "opt-in" is the only method that ensures users are not tricked into allowing their personal information to be sold and exchanged without their intentional consent.

Part #3 gives web site operators some measure of accountability for their actions as well as those of the third party companies they buy and sell profiles from. Many companies insist they have absolutely no control over the data once it leaves their offices, which may be true. However, the lack of control may in fact be due to disinterest in what the third party does with the data, and not because they have lack leverage. Contracts made between the companies governing the type, frequency, and quality of data could also include usage clauses protecting the individuals whose data is exchanged.

One alternative bill before the U.S. Senate that has garnered much media and industry attention is the Secure Online Communication Enforcement Act of 2000 (2000 5.2063), sponsored by Sen. Robert Torricelli and Sen. Russell Feingold. A more controversial bill than its above counterpart, it would require web sites to provide "opt-in" controls instead of leaving the choice between either "opt-in" or "opt-out." Its more strongly worded language also includes clauses to ensure it pre-empts any state legislation, and prevents websites from denying access to individuals who choose not to allow their personal information to be disclosed.

Other bills are also pending, including a similar bill in the U.S. House of Representatives. Sponsored by Congressman Vento and named the Consumer Internet Privacy Protection Act of 1999 (H. R. 313), it aims to accomplish many of the same goals as the two Senate bills cited above. Importantly, this bill would require any interactive computer service to provide users with access to their personally identifiable information, permit verification and corrections, if necessary. While control over the information is important, this bill takes the extra step to ensure that individuals have the right to correct any potentially damaging information about them.

These propositions all cover important ground towards completely protecting online privacy. However, none besides the Children's Online Privacy Protection Act has yet to be ratified by either the House or Senate. The government has held off enacting legislation in part because of the hope that self-policing by Internet companies will occur. However, while Congress and government agencies wait, the public suffers daily from innumerable privacy violations. The number of victims can only increase with time.

Conclusion

The practice of user profiling in and of itself offers a number of useful features, and when used properly can provide both users and businesses with a more rewarding online experience. However, the risk of impropriety is simply too high when online user profiles are combined with highly detailed direct- marketing databases. As previously shown, the potential for improper use is definitely present and significantly overrides any benefits that could be derived from a business standpoint. To strike a balance between over-zealous privacy protection and the needs of enterprises, web sites should adopt and adhere to the following privacy code:

- ✓ When requesting sensitive user information, clearly explain in plain English the reasons and uses (both internal and external) for the data.

- ✓ Provide users with the option to allow their data to be distributed to third parties, preferably as an "opt-in" rather than "opt-out" option.
- ✓ Allow users to review all the information in their profile, verify it, and correct as desired.
- ✓ Notify users when any changes occur affecting the use of their personal information.
- ✓ Not restrict access for those users that do not permit their information to be sold or otherwise exchanged.

While many Internet businesses insist that government intervention would only stifle the innovation and growth of the Internet, it must be pointed out that the government also has a duty to protect the rights of its citizens. Therefore it should hasten to enact comprehensive legislation protecting the online privacy rights of its people, and either instruct the FTC to administer such protection or authorize the creation of anew agency for such a purpose. While this may seem too legislative to some, part of the responsibility of a society is to guard the well being of the people, which in some cases necessitates explicit government intervention. Given the risk of abuse and the potential repercussions, it only makes sense that the government take an active role in safeguarding privacy.

Sources

1.http://web.lexis-nexis.com/universe [several queries that did not scan properly]

2. http://bwarchive.businessweek.com

3. http://www.ftc.9ov/oRa/2000/01/reverse4.htm

4. http://www.whitehouse.aov/WH/SOTUOO/sotu-text.html

6. http://www.doubleclick.net/company_info/press_kit/pr.00.03.02.htm

7. http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf

8. http://www.epic.org/privacy/internet/EPIC_testimony_799.pdf

9. http://osecnt13.osec.doc.gov/ecommerce/barriers.nsf

10. http://www.ftc.gov/bcp/conline/pubs/online/kidsprivacy.pdf

11. http:/ /www.epic.org/reports/surfer-beware3.html