

The Business Ethics Center of Jerusalem

ONLINE HI-TECH MAGAZINE: Consumer Privacy on the Net

Introduction

In George Orwell's novel 1984, every citizen is under the constant surveillance of the government. At every street corner, on every building, and on every wall there is a reminder that "Big Brother is Watching You." Every move a person makes is recorded by the ever-present telescreen. Orwell wrote his novel not as a fantasy about what life could be, but as a warning of what it is becoming.

At any given moment, web users are being spied upon by the websites they peruse. Companies say that online profiling, also known as data mining, helps them to serve their consumers better. This spying enables companies to tailor their websites so that their consumers see exactly what they want. Although this monitoring seems beneficial to the consumer, Internet users are afraid that websites know too much about them. Eighty four percent of Internet users are concerned about businesses or strangers finding out personal information about themselves or their families. Companies often know more about the consumer than they know about themselves.

Important Facts about Consumer Privacy on the Internet

- **75 out of the 100 most popular Web sites** collect personal information, even though 40 of these lack complete privacy policies. (Red Herring, September 1999)
- The U.S. Federal Trade Commission reports that **80% of all websites** do not use industry-accepted fair information practices such as informing users about data collection and letting them opt out of providing data.

As efforts to spy on consumers on the Internet grow, so do peoples' fears about the spying:

- **Two-thirds** of Americans say Internet companies should **not be allowed to track users' activities**
- Seven in ten Internet users (71%) say that **Internet users should have the most say** over how Internet companies track users' activities. (The Pew Internet & American Life Project)

What are the Ethical Problems?

The following are some of the main problems, all of which could be considered breaches of privacy:

1. Basic Privacy: People don't want strangers to know anything about them.
2. Consent: Web sites gather most of their personal information without notifying

the consumer.

- 3. Use of the Information: Companies that inform the users often don't explain how they will use the information.
- 4. Information Sharing: Web sites often share information with each other, which is a clear breach of confidentiality.
- 5. Context: The activities of an individual could be taken out of context and be used to inaccurately define the individual or his ethnic/religious/social group.
- 6. Coercion: People do not provide information about themselves willingly, but only to gain a desired online service, free gifts, etc.
- 7. Control of Personal Information: Personal information is a valuable resource, and the individual should be able to decide who has access to his information and how it is used. When a company knows all of an individual's personal information, the individual loses his power over it.
- 8. Theft of Credit Numbers & Identities: Credit card theft occurs when hackers break into a retail website, and steal customers' credit card numbers. Identity theft occurs when a thief steals a person's social security number, driver's license number, accounting information, etc., and uses these to imitate the person. The thief can then open up fake bank accounts, credit cards, etc.

Companies are able to build a detailed profile of an Internet user from his or her activities across several websites. The profile could include information about the consumer's purchases, investments, health concerns, etc. With this information, a company can create a complete picture of the identity of the individual, which can be exploited by the company or by others.

Infamous Cases

The Internet is still in its infancy, and therefore lacks basic laws of proper behavior. Companies stumble in the darkness in this absence of online ethics & etiquette, gathering information in ways that the public later judges to be unethical. When the media reports on companies going too far in gathering information online, panic spreads amongst Internet users, who are fearful of the increasing encroachment of companies into their privacy and liberty.

The most well known example involved DoubleClick, one of the largest advertising companies on the Internet. DoubleClick runs advertising banners that can be seen on many websites, telling users about other sites they might want to visit. When a user clicks on a banner to go to another site, DoubleClick tracks their movements, creating a record of their online behavior. The story made headlines when it was found that DoubleClick was creating a database combining records of millions of users' online behavior with their real world identities and postal addresses. This would provide advertisers unprecedented knowledge of a person's identity and spending habits, along with easy access to the person. Amidst U.S. Federal Trade Commission pressure and in the face of numerous lawsuits, the company decided to put the creation of their database on hold.

Another famous case in the U.S. involved online retailer Toysmart.com. When the retailer announced that it was going out of business, it offered to sell its consumer database containing the confidential information of hundreds of thousands of customers. The company, under U.S. government pressure, withdrew the offer. Two other Internet

retail sites, Boo.com and Craftshop.com had attempted to do the same.

Numerous other well-known websites have been accused of stalking customers and secretly gathering information about them. A lawsuit in Texas accused Yahoo of stalking, due to its electronic monitoring of the browsing habits of its customers. AOL and Netscape have come under fire for tracking downloads of files from the Internet. In another prominent case, ToysRUs and several other large online retailers were found to be sharing data about online consumer behavior with each other.

Perspective from Jewish Sources **by Rabbi Dr. Asher Meir**

INTERNET PRIVACY

The promise of the Internet comes from its ability to tie together hundreds of millions of people in a unified worldwide forum. Finding just the right person, product or piece of information now takes a few minutes and a few cents, where only a generation ago it would have taken months and eaten up an enormous budget.

However, this promise comes at a great cost in privacy. Just as I can peer into the windows of a hundred million virtual houses to find what I am looking for, so can a hundred million others peer into my own virtual home. There is an unimaginable increase in the amount of information gathered, the ability to aggregate and analyze it, and its accessibility. If I visit agathiechristie.com and then check out the baseball scores, within a few minutes a banner could appear on my screen advertising the new thriller set in the world of sport.

FOCUS ON CONSENT

The debate over Internet privacy has been mainly focused on the subject of consent. There is general agreement that users have a right to keep information about themselves private; the main question is how they are to go about doing so. One possibility is an "opt-out" policy, in which all information is considered public unless the user explicitly expresses his desire to keep it private; the other is an "opt-in" policy in which service providers may collect information only when explicitly permitted by the user.

Many advocates, while accepting the basic focus on privacy, think that consent is not the solution and that regulations are required. They suggest that an "opt-out" policy is problematic because it involves minimal consent. And even an "opt-in" policy may lack adequate consent: Perhaps the consumer lacks enough information to give truly informed consent, or perhaps there is a degree of coercion because withholding consent has negative consequences, such as limited access to service.

PRIVACY VS. MODESTY

Judaism certainly shares this concern for privacy. Our tradition establishes a very high standard of discretion, a universal "opt-in" policy where all communications, even personal ones, should generally be considered private unless the speaker permits revealing them. The Chafetz Chaim writes, "When someone says something to his fellow, it is forbidden to reveal it unless the speaker gives him permission."

But a Jewish perspective would widen the focus. Judaism considers not only privacy but also modesty. Privacy refers to what I would prefer to keep hidden, while modesty refers to what normatively ought to remain hidden. Forcing me to go to work in a bathing suit would violate my privacy, but even if I dress this way willingly there is a breach of modesty. Indeed, Jewish law asks us to avert our gaze if we see someone engaging in a private activity, even an innocent activity which is not being concealed. Rav Shneur Zalman of Liadi writes, "Neighbors need to be as careful as possible not to look at each other's activities in their common courtyard."

Breaches of modesty, no less than breaches of privacy, can be very destructive to society. Exposing people's personal habits ultimately creates a busybody atmosphere where everybody is minding everybody else's business, leading to an unhealthy homogenization and degradation of standards. In addition, scrutiny damages our sense of dignity and restraint.

Our Sages, recognizing these considerations, say that if someone is determined to commit an immoral act, he should at least do so in utter secrecy. Then the act won't contribute to public brazenness, and the individual will find it easier to correct his behavior, since his public image is unaffected.

Our tradition reminds us that it is not enough to ask what human beings want; we also need to concern ourselves with who human beings are. Character development, both personal and public, requires the shelter of modesty; it cannot take place in the spotlight of surveillance, however unobtrusive. We should strive to introduce these humanistic and spiritual dimensions into the public debate on Internet privacy.

SOURCES: "Opt-in": Yoma 4b; Chafetz Chaim 9:6 and Beer Mayim Chaim 2:27. Not to spy: Rema in Shulchan Arukh Choshen Mishpat 154:7, Shulchan Arukh HaRav Nizkei Mamon 11. Acting in secrecy: Kiddushin 40a and commentaries.

Rabbi Dr. Asher Meir is the Director of the Jewish Business Response Forum, at the JCT Center for Business Ethics. The response forum welcomes questions by business managers. For more information, email Rabbi Meir.

How do companies gather information about you online?

There are numerous ways for companies to gather information online, without people knowing it:

Cookies: Every time a person goes to a particular Web site, the site records critical information about the person (user's name, email address, type of browser, credit card number in the case of a purchase, etc.) This information is stored as a cookie on the person's computer, so the website can access the information when the person returns to the site. Cookies make it easier for people to browse the web, by eliminating the need to input information repeatedly, and by speeding up purchases (for example through the use of shopping carts and web pages which can recommend items based on the person's spending habits). Cookies are used by nearly every commercial website.

Web bugs: Many websites include invisible images called web bugs, which secretly lurk in the background while a person peruses the site, gathering information on the person. Web bugs allow a site to identify the IP address of the person's computer (clearly

identifying their Internet Provider, university or company, and thereby their location), the type of computer being used, the person's name and email address, etc. This information is then transmitted back to the website or to another company. Web bugs are used less frequently than cookies, but are growing in popularity.

Personal Input: People provide much information about themselves, when registering on websites, ordering information online, etc. Companies coerce consumers into providing information on themselves by offering them free products, telling them they must register to gain access to the site, asking the consumer to fill out a survey, etc.

Solutions

There have been many solutions proposed to the ethical problem of online data gathering, but none has yet been widely accepted by companies and web users. One of the reasons that they are so many proposed solutions, is that consensus has not been reached yet as to who should be doing the monitoring. Companies argue for self-regulation through industry groups. Consumer advocacy groups oppose this idea, and say that companies cannot be trusted. People have also put their hope in governments to protect them. Briefly presented below are a few proposed solutions:

Industry Self Regulation

Companies argue that they should be allowed to write ethical guidelines for online data gathering, since they are most informed about new technologies. Consumer advocacy groups ridicule this idea, because of its inherent conflict of interest.

Proponents of industry self-regulation also say that companies will be more willing to accept laws that are proposed by groups within their industry. One example of industry self-regulation is a plan that was proposed by the Electronic Commerce and Consumer Protection Group, composed of eight prominent companies with online interests (including AOL and Microsoft). The group recommends that websites follow the following guidelines: 1. Companies should provide notice to consumers as to what type of information is to be collected and how it will be disseminated, 2. Merchants should provide consumers with choices as to the dissemination of information to third parties. 3. Merchants should provide consumers with reasonable access to the records of the individual consumer. The U.S. Federal Trade Commission has proposed a set of guidelines very similar to this, adding that companies need to protect the information that is collected from consumers.

Consumer Advocacy Groups

Several advocacy groups sponsor websites that notify the public when Internet privacy abuses occur by companies. (Several are mentioned in the links section, below) These whistleblowers are knowledgeable about the issues and are impartial. However, a small online organization with little staff and no power to punish lawbreakers would be ineffective against powerful offenders.

World Governments

The ability of any single world government to regulate the online actions of companies is limited because the Internet spans the entire planet. In addition, governments are typically slow to implement new technologies, and therefore would find it difficult to monitor fast-moving Internet companies.

The U.S. Federal Trade Commission and major online advertisers in June agreed upon a plan to limit their activities, relying on the "opt-out" option. Under this option, companies are allowed to gather information on a person, unless the consumer explicitly requests that the company not do this. An "opt-out" plan puts all of the responsibility on the consumer, who is often ill informed about online data gathering, and therefore unable to protect himself. The deal also gives the FTC little power to punish wrongdoers.

Recent laws in the European Union go further than the FTC plan, relying on an "opt-in" plan. (Under an "opt-in" plan, a company can gather information on a person only if the person gives permission for the company to do so.) The laws also say that info gathered for one purpose can not be disclosed for another purpose without the consent of the individual.

Until everyone agrees on a reliable standard to protect consumers' rights on the Internet, it is up to consumers to protect their own rights. What can consumers do?

- 1. Consumers should be aware of the existence of cookies on their computers, and should only accept cookies from a limited number of trusted websites.
- 2. Users should limit the amount of information they willingly provide to companies.
- 3. Consumers can also use an anonymous web browser (available for download from the World Wide Web), that allows one to surf the web without providing information to companies, and to use confidential email programs that allow only the intended receiver to open the email.