Privacy In The Internet Age - Illusions, Reality and the Preservation Of

Onyemaeki Akaeru

Vincent Rampello

Cameron University

Abstract

Individual users who expect privacy or anonymity on the Internet must know the reality. For individuals wanting to secure their privacy online, they first must understand how privacy is regulated under the law, how business views the information they gather on individuals and what business does with the information. Only then may they take effective action either individually by using tools that help preserve privacy, or collectively by applying pressure to their government to preserve their privacy online.

Privacy: Users' Expectations Versus the Reality on the Internet

Consumer privacy issues are a "red herring." "You have zero privacy anyway. Get over it," said Scott McNealy, Sun Microsystems CEO to a group of reporters, 1999. This statement, more than any other, epitomizes the dichotomy between consumer expectations of privacy as they utilize the Internet and the attitudes of business towards the information they gather from consumers and customers Internet use.

The reasons for the difference in viewpoints where consumers expect their Internet usage is their private information and how business sees the information gathered from that usage as an asset to be bought, sold and leveraged in business operations are many. They stem from both a lack of consumer knowledge of business practices and the laws that govern those practices, as well as technological advancements on the Internet. This paper examines the differences between consumer and business privacy expectations, the reasons for the differences, the advancements in technology that have exacerbated the issues of what privacy both is and exists on the Internet, how the laws governing privacy have not kept pace with technological advancements, and what can be done by users as individually and collectively to preserve their privacy.

Previous Work

The willingness of individuals to disclose private information varies as a balance between individuals' privacy concerns versus convenience and perceived added value of services (Chellappa & Shivendu 2007). While individuals may implicitly agree to disclose private information for a business's internal needs, they do not automatically agree to the sharing of private information between businesses without their consent (Pollach 2005). The cost-effectiveness of tracking consumer behavior on the Internet allows for unprecedented real-time scrutiny of individual activity. Prior to the Internet, the amount of information that could be reasonably collected was limited in scope and was available only in the aggregate (Cronin 2000). The demand by individuals for privacy as a response to companies seeking to sell the information gleaned through data mining operations has produced differing outcomes. In the European Union, the outcome has been laws and regulations that govern the use of private information. The United States has taken a more laissez-faire approach consistent with its more capitalistic society and "encouraged a privacy policy of self-regulation". This has resulted in online privacy statements that exists primarily to protect the companies that issue them from lawsuits while simultaneously permitting the company to maximize profit by usage or sale of the information it gathers from individuals that interact with the company's online presence (Fernback & Papacharissi 2007).

Although privacy is not specifically mentioned in the United States Constitution, the US Supreme Court has consistently taken the point that the right of individuals to privacy as "the right to be left alone". Privacy in the Internet age has expanded to mean "a person's right to control information about him or her". However, "federal regulation of private information practices is uneven at best and applies only to certain kinds of records." (Langenderfer & Miyazaki 2009)

Users' expectations of privacy and anonymity - The illusion and the reality

The illusion that privacy exists convinces people to trust the Internet and its services. Internet users share information with online service providers blinded by the illusion that they control all they share, how it is used and what gets deleted. Facebook provides a privacy setting page where users can choose who gets to see what and who doesn't. With this provision every Facebook account holder falsely believes they can add, access and delete information with no worries of it been made available for viewing by a third party. The reality is when a web user has provided his personal data to complete a transaction; the power for controlling his data has been transferred to the vendor. The original owner of the data, the web user, can only hope the vendor will handle the information properly and protect his privacy. (Facebook and your privacy, 2012)

Companies have always collected information on their customers and potential customers. The information they manage to collect is considered an asset of the company to be used in marketing to customers or for sale to other companies. Even information that a customer considers private but necessary to release to a company in order to do business becomes the property of the business to do with whatsoever it pleases. (Nemzow, 2012)

The reason why Internet users' expectations are different from the reality is this; the so called companies who pretend to exalt privacy make their money by controlling vast amounts of their users' information. Whether through targeted advertising, cross-selling or simply convincing their users to spend more time on their site and sign up their friends, more information shared in more ways, more publicly, means more profits. This means these companies are motivated to continually lower down the privacy of their services, while giving users the illusion of control. Privacy policies are deliberately written in legal language that is

hard to understand by the average user, and the terms are frequently changed to benefit the companies with no notice given to users or customers. (Pollach, 2005)

The online advertising industry has built its business model around unrestricted access to our personal information and they work vigorously to get it.

Actual privacy on the Internet - User tracking in aggregate

Have you ever wondered why when you access a website on the web all you see are ads that show products that you have viewed or products related to what you have viewed. It is not a coincidence that you see ads tailored for your eyes specifically.

The old way advertising companies tracking Internet users is via cookies and storing the information in categories in aggregate is giving way to methods to track individuals.

When a company that wishes to advertise on the Internet, it buys access to the advertising companies ad server that will serve its ads only to the categories of user profiles that match the categories the company has purchased ads for, but does not get the information on the user's profile.

Businesses are taking marketing too far; the general public has very little idea that every second they are on the Internet, their behavior is being tracked and used to create a profile. These profiles of individuals, constantly refreshed, are bought and sold on stock-market-like exchanges that have sprung up in the past 18 months. WSJ (2010) study found the following: The nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning. A dozen sites each installed more than a hundred. The nonprofit Wikipedia installed none. (Angwin, 2010)

Pushing the limits - Business tracking of individual users

In addition to generalize aggregate tracking of users, companies are also tracking or attempting to track individual users online, with personally identifying information that a user considers private, but is has given to the company in order to do business with or access the services provided by the company.

An example of a company that tracks internally is Amazon. The company knows who you are after you have created an account with them, what web pages you have visited on the site, what you have added to wish lists and/or placed in your shopping cart, and what you have purchased. It uses this information to make recommendations of products you might be interested in purchasing. Most if not all users would consider this an acceptable use of personally identifying information by a company so long as the information is kept secure and is not released to third party companies.

An example of limited sharing is when a bank rents access to a life insurance company its list of users in with minimal personally identifying information in accordance with both its privacy policy and the applicable laws governing release of personal information to third parties. Users can opt out of certain disclosures of personal information in accordance with the bank's privacy policy and the laws governing the release of personal information, but only as long as they continue to do business with the bank. After ceasing to do business with the bank, the disclosure of personal information to third parties is governed by what the user's choices to limit release of personal information under the bank's privacy policy when they were customers of the bank. (Graham-Leach-Billey Act, 1999)

An example of the unlimited sharing is Facebook. The company collects personal identifying information on its users as a requirement for accessing and using the site as part of the sign up process. It continues to gather information on its customers by tracking their likes,

friends and follows. Since most users remain logged in to the site after leaving it to visit other web sites, if those web sites have a Facebook widget, Facebook will know what individual user visited what pages at what sites and when they were visited. This combines the information Facebook receives directly on the social networking site directly with the information that was previously only available in aggregate to advertising companies like DoubleClick. (Facebook and your privacy, 2012)

This is one of, if not the ultimate personally identifying information databases. Facebook has attempted to sell this information to third parties but has partially backed down for the time being due to user backlash. However in order to remain in business Facebook has to monetize its user base so it is only a matter of time before Facebook sells the information in whole or in part. They continue to modify their privacy policy in order to make it easier for them to be able to sell personally identifying information to third parties, and harder for users to opt out of disclosing the information. (Facebook and your privacy, 2012)

A frayed patchwork - Laws regulating privacy fall behind as technology races ahead

There is no comprehensive law in the United States that regulates the collection, storage, transmission, or use of personal information on the Internet. Congress should enact a baseline consumer privacy law, says Leslie Harris, the president of the Center for Democracy and Technology, a public policy group that promotes Internet freedom. “We’ve been trying to get a comprehensive privacy law for over a decade, a law that would work for today and for technologies that we have not yet envisioned." (Singer, 2013)

The majority of the existing privacy laws were passed way before the Internet became a hub for financial transactions and social networking. A few common Internet privacy laws are:

the Online Privacy Protection Act of 1999, the Consumer Internet Privacy Protection Act of 1999 and the Personal Data Privacy Act of 1999.

Future Work: To preserve privacy in the Internet age - Individual responsibilities, and need for government action

The privacy of individual users of the Internet can partially preserved by first understanding to what extent companies are willing to go obtain information on their customers and potential customers. Once individuals understand what companies do to obtain their information, they can utilize tools to deny those companies the information they are seeking. A good rule of thumb for users to determine if a company will only collect the minimum of information they need to interact with their customers and safeguard the information they do collect is to examine the company's privacy policy. If it is hard to locate, difficult to understand, or does not appear to limit what the company can do with information that is disclosed to it, the company should not be trusted to do right by the individual consumer.

To preserve Internet privacy while browsing requires some precautions on the part of the user. Some of the more effective tools for preserving Internet privacy are available for the Firefox web browser in addition to the privacy tools built into the browser itself. Tools included in the browser include the Do Not Track setting where individuals can indicate to companies that they do not wish to be tracked, and the ability to choose not to "Accept third party cookies", or decide how to manage them. Add on tools to preserve privacy include AdblockPlus and the closely related Adblock Plus Pop-up Addon to block advertisements from loading, BetterPrivacy to manage Flash LSOs otherwise known as Flash cookies, Ghostery for cookie and web tracker management, and NoScript to manage the use of scripting by websites. (Firefox, 2013)

However, in order for the tools above to preserve privacy, they have three additional requirements: 1) A user who understands that most companies would like to have no limits to what information they collect from individuals and would not like to be held responsible for what information they have collected, 2) A user who trusts the makers of the tools not to abuse the responsibility to preserve the privacy of individual who uses the tools, and 3) a certain amount of technical ability of the user to successfully install, maintain and utilize the tools.

It is the requirements for users to understand that most companies would gather as much information as possible without having limits on what they can do with what they can collect, and that most users do not have the technical ability to use privacy tools responsibly, that drives the need for government action in the United States that the European Union has already pioneered. If individuals desire that their privacy be respected and safeguarded they should let their leaders know where they stand on the subject. Otherwise the laws will be written to favor companies at the expense of the users, as the recent attempts to pass the to Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) demonstrate.

To let your legislators know where you stand, individuals should start by contacting them. Individuals can find out who their US Representative is and how to contact them at www.house.gov, Senators at www.senate.gov. President Obama is committed to creating the most open and accessible administration in American history. That begins with taking comments and questions from you, the public, through this link: http://www.whitehouse.gov/contact/submit-questions-and-comments.

References

Angwin, Julia (July 30, 2010) The Web's New Gold Mine: Your Secrets, WSJ Online http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

Chellappa, R. K., & Shivendu, S. (2007). An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization. *Journal Of Management Information Systems, 24*(3), 193-225

Cronin, M. J. (2000). Why Internet Privacy Matters to Consumers. *Consumers' Research Magazine, 83*(9), 16

Facebook and your privacy (2012) Retrieved 19 April, 2013 from http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm

Fernback, Jan & Zizi Papacharissi, Zizi (2007) Online Privacy as Legal Safeguard: The Relationship Among Consumer, Online Portal, and Privacy Policies New Media & Society October 2007 9: 715-734, doi:10.1177/1461444807080336

Firefox Privacy and security settings Retrieved 19 April, 2013 from http://support.mozilla.org/en-US/products/firefox/privacy-and-security

Graham-Leach-Billey Act: Privacy of Consumer Financial Information (1999) Federal Trade Commission http://www.ftc.gov/privacy/glbact/glboutline.htm

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the Information Economy. *Journal Of Consumer Affairs, 43*(3), 380-388. doi:10.1111/j.1745-6606.2009.01152.x

Nemzow, Martin (2012) Who Owns Customer Information? Baseline Retrieved 19 April, 2013 from http://www.baselinemag.com/c/a/Security/Who-Owns-Customer-Information-491502/

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal Of Business Ethics, 62*(3), 221-235 doi:10.1007/s10551-005-7898-3

Singer, Natasha (March 30, 2013) An American Quilt of Privacy Laws, Incomplete *The New York Times* Retrieved from http://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html?pagewanted=all&_r=0

Bibliography

FTC (March 26, 2012) FTC Issues Final Commission Report on Protecting Consumer Privacy, NativeWeb http://www.ftc.gov/opa/2012/03/privacyframework.shtm

FTC (March 2012) Protecting Consumer Privacy in an Era of Rapid Change Recommendations for Businesses and Policymakers, PDF http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

Halbleib, Jennifer (April 8th, 2010) Modernizing Privacy in the Internet Age, NativeWeb http://futureoftheinternet.org/modernizing-privacy-in-the-internet-age

Reynolds, Glenn Harlan (n.d.) Privacy in the Internet Age: Time to Go? NativeWeb http://rebooting.personaldemocracy.com/node/5492

Rogers, Zach (January 23, 2013) Product Manager David Baser on Facebook's Attribution Roadmap, NativeWeb http://www.adexchanger.com/social-media/product-manager-david-baser-on-facebooks-attribution-roadmap/

Sprenger, Polly (January 26, 1999) Sun on Privacy: 'Get Over It', NativeWeb http://www.wired.com/politics/law/news/1999/01/17538

Troianovski, Anton (June 18, 2012) New Wi-Fi Pitch: Tracker Network Developers Offer Retailers Ways to Keep Tabs on Customers as They Shop, NativeWeb http://online.wsj.com/article/SB10001424052702303379204577474961075248008.html

Walter-Echols, Michael (February 27, 2009) Panopticon – Surveillance and Privacy in the Internet Age, NativeWeb http://www.wpi.edu/Pubs/E-project/Available/E-project-022709-132355/unrestricted/Panopticon.pdf

The White House, Office of the Press Secretary (February 23, 2012) Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights, NativeWeb

http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

Wikipedia (December 27, 2012) Privacy, NativeWeb http://en.wikipedia.org/wiki/Privacy

Wikipedia (January 14, 2013) Electronic Communications Privacy Act, NativeWeb http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act