Place for Privacy to Hide in E-Commerce Age

October 27, 2008

Abstract

With the increasing ease of data availability and development of technology of search engine, more and more concerns are casted into privacy issues in the Internet service such as e-commerce. There are two kinds of different attitudes towards privacy on the Internet. One is pessimistic, in which privacy is already or to be dead finally. The other is optimistic, in which privacy could also find its own space to live. The main reason for the argument is that how to balance privacy of customers and convenience of service in the Internet, especially in e-commerce.

We take the position that privacy is not dead even in the environment of highly developed Internet. As argument, we try to figure out three reasons that cause privacy violation in the on-line environment and then we argue about these three reasons to eliminate privacy violation in the Internet. And then we show many aspects of efforts towards privacy protection in online environment. Finally, according to the discussion, we predict the future direction for the development of privacy in on-line environment.

1. Introduction

With the development of technology and Internet, on-line ecommerce is becoming more and more important way of shopping for people. However, along with the convenience that you benefit from the on-line ecommerce, your personal information related to your shopping habits, interests, and things like this would be exposed to the service provider, who collects these kinds of information in the hope of offering more convenient service for customers in future. There are two ways for service provider to collect customer information. One is to ask customer to fill several questionnaire forms, such when customer register to be a membership of a website. In some cases, website offer bonus to exchange user's information. The other is to employ network tools to collect, record, and even discover personal information about customers. As its potentiality, people would be likely feel uncomfortable when treated by the second method. After collecting personal information, the service provider would be able to provide more precise stuffs and recommendation for every customer when visiting the websites. The more personal information is provided, the more likely website provides exact goods to customers, and as a result, people would be more likely to spend money. Amazon [1] is the first web service provider that introduces such kinds of service. The incident occurred in 1991 when Amazon.com employed purchase circles, an online marketing tool that, supposedly for the customer's benefit, revealed what books Amazon's customers from some well-known corporations were buying, which you can also find out presently. For example, a client who decided to buy a book about the principle of operating system would likely also be interested in Linux concerning books. The usability of personal information improve our lives and save our times. For company, these tools dig out the potential purchase of customer from their current buying behavior and increase the chance of customers buying products in one website, so after amazon, many online manufacturers began to provide the recommendation services on their websites.

However, the high speed at development of e-commerce, database technology, and improvement of search engine in precise and speed arise people's concern about privacy problem in online environment. The more technology develops, the more likely, people could identify others in today's online environments. On the other hand, the more you participate in e-commerce, the more you register in the Internet, and the more you use search engine, the easier you would be identified by others in the Internet. As technology seems not be tired of moving forward, some people afraid that privacy of online users would be totally detroyed and would be dead , or at least will die soon under such tendency.

We can not deny the concern about this issue.

Indeed, nowaday's technology exert threats to the privacy of online users. However, people, who thought that privacy would be dead as a result of the development of technology, is go too far from the issue. We cannot agree with this opinion since it only focuses on the negative aspect of the development of technology. It ignores other aspects that would influence users' online privacy.

2. Counterclaim

2.1 General Idea

"You have zero privacy anyway,"

"Get over it."

Above are comments from McNealy, CEO of Sun corporation who is an advocate of the opinion of "Privacy is dead". In [4], the author argued that technology that provide convenient to our life, seems to encroach our personal privacy at the same time. The same streaming video technology that allows grandma and grandpa to chat with their grandchildren is being used to spy on employees in the workplace. Simson Garfinkel[3] in his excellent and severely under-appreciated book, "Database Nation." said that "We know our privacy is under attack," "The problem is that we don't know how to fight back." Privacy would be dead finally. Garfinkel says we need to rethink privacy in the 21st Century. "It's not about the man who wants to watch pornography in complete anonymity over the Internet. It's about the woman who's afraid to use the Internet to organize her community against a proposed toxic dump - afraid because the dump's investors are sure to dig through her past if she becomes too much of a nuisance," Garfinkel writes.

As the problem is so pressing now, are we aware of this problem in privacy now? "Millions of American consumers tell us that privacy is a grave concern to them when they are thinking about shopping online," Bernstein said. If this is the case, why could we take measurement to stop privacy being dead procedure, but still in the environment which would be worse? Reasons are as follows.

Firstly, using personal information to serve certain individual would provide better service and save time for customers. For example, you are looking for racquets to play tennis, you browser several pages in Amazon, compare the quality of racquets and their price. Finally, you decide to buy one. When you check out, you would find several items related to tennis recommended by Amazon for you. With this help, you can buy a suite of equipments for tennis, including apparel, shoes, and balls besides only one racquets. One search but you can get the whole things you need. For some people, they would like to give up their personal information to e-commerce provider to gain convenience and time savings. However, there are people who trade their personal information with little convenience due to their unawareness of the privacy problem.

Secondly, company would never stop their pace to mine the personal information of customers in order to share a large part of market in future business. We are not at the age of mass product. Individualism is a symbol for our current society. People are eagerly to be distinguished themselves from others. Personalization service is a trend in future business. Before the appearance of Internet, it is not convenient for people to customize their product since you need to stop by the company to tell them what you want. However, with the help of Internet, now many companies take advantage of the Internet to provide a web service for customer to customize their own style products. Such as Nike.com[8] now provide a way for customer to customaries their own sneaker. Lenovo[9] let user to assemble their own labtop. As long as company wants to provide personalized service, they would be more potentially to collect personal information about customers as much as they could. This is the main cause of the privacy violation in ecommerce world.

Thirdly, the improvement of technology forced by company or research group for better life would be the fundamental reason for encroachment of privacy. Common technology to collect customers personal information includes cookies and web bugs[7]. Cookies collect information as user surfs the web and feed the information back to a web server. An online vendor's site will send cookies (which are most simply an identification number) to a user's computer, where it is stored in a file on the user's hard drive and serves as a digital identifier tag that notifies the vendor whenever that user re-enters the vendor's website. Although users can configure their browser to disable cookies, some sites require users to accept them before allowing entry. Web bugs are images--usually invisible because they are only one pixel wide by one pixel high-that are embedded in web pages and HTML-formatted emails. Advertising networks often use web bugs on web pages to add information to personal profiles stored in cookies and to collect statistics about how many hits the site gets. Ad networks also use web bugs in "junk email" campaigns to determine how many users read the emails and visited the linked site, to remove users from the list who did not open the marketing emails at all, or to synchronize cookies with the user's email address.

Cookies and web bugs are only the beginning of technology used for privacy violation. The rise of e-commerce enables marketers of all stripes to capture bits and pieces of our buying and Web surfing habits. Database technology enables those bits and pieces of your daily life - the matrix of your personal world - to be assembled and repackaged thousand of ways and sold to anyone wanting to target you for a quick sale or an unwitting scam. These are the darker angels of the digital age which would bring diseaster to user's online privacy.

In addition, as the United States and other governments have been initiating increasing numbers of surveillance programs in the name of fighting terrorism, the possibility that information stored for use in ecommerce personalization may find its way into a government surveillance application is becoming increasingly real. This kind of government behavior is hard to notice by customers.

Furthermore, in wireless area, mobile device could gather user precise physical location. Many wireless phone manufacturers therefore incorporated Global Positioning System (GPS) technology, which uses satellite signals to track a user's location, inside the handsets of their new models. This would benefit for people who are not good at direction, but privacy problem would arise at the same time. Privacy advocates have argued that wireless GPS will allow large telecommunications companies to track customers' movements [10].

Intentially leak of privacy by customers, potentially record and gather personal information by company, and the powerful technologies using in identification people on the internet, contribute to the worse and worse environment of customer online privacy. But, are these elements enough to totally destroy privacy? The answer is no. In the rest of this section, we refute each kinds of elments on its ability to destroy the privacy.

2.3 Intentially Privacy Disclosure by Customers

Indeed, people would trade some personal information for convenience and savings. But the question is that such are these convenience and savings worth the personal information? How many people would be unaware about their privacy? Ackerman in [5] classified people into three groups:

- The Privacy Fundamentalists who almost refute to provide personal information even in the presence of privacy protection measures.

- The Pragmatic Majority who constitute the majority of the Internet users, who exhibit privacy concerns, but not as strongly as the Privacy Fundamentalists.

- The Marginally Concerned who almost always are willing to reveal their personal data. Furthermore, in Spickermann et al.[9], it is shown that the Pragmatic Majority class contains two “subclasses”, namely those whose main concern lies in revealing personal data, such as name, address, etc., and those whose main concern is about providing information concerning their personal profile(health interests, etc.).

Based on the classification, the results of previous Westin surveys are summarized in Table1[11]. From this table, we can see that in the past eight years, people with privacy unconcerned are reducing, while people become privacy pragmatists is increasing. The results is promising for the privacy protection. As people become more and more concerned about their privacy, they would consider more carefully when making the choice between exposing personal information and gaining convenient service.

Year	Privacy Fundamentalist	Privacy Pragmatists	Privacy Unconcerned
1995-1999	~25%	~55%	~20%
Mid 2000	25.00%	63.00%	12.00%
Late 2001	34.00%	58.00%	8.00%
2003	26.00%	64.00%	10.00%

Table 1: Westin Privacy Classifications for previous surveys

2.4 Efforts by Company

It is true that when customer using e-commerce such as buying books in Amazon.com, the service provider would keep a track on your behavior, store information about your personal information. The more you buy, the more information they would gain. This is unavoidable. However, we do not deem data availability by the company as privacy violation. Because the data collected by company is good for the usability and could be useful for better service to customers. Privacy violation is not because of the data collection by company, but data abuse. Does company have the right to abuse customers’ data at will? Here are several lawsuits about the company that abuse customers data.

- EBay disavows the responsibility for privacy violation(Recent reports show that China's TOM-Skype platform, a joint venture between China-based TOM Group and eBay uses a sophisticated monitoring system that scans and stores private chat messages for conversations and keywords deemed a threat to government of China.)[6]

- AT&T modify its polidy to requires several million users of its Internet and video services to acknowledge that AT&T owns their account information. It also states that this is a clarification of its pre-existing privacy policy -- not a new policy. Privacy advocates view AT&T's ownership claim as a bold new move designed to further erode privacy rights. Now, AT&T is faced with a lawsuit filed by the Electronic Frontier Foundation claiming that it violated customers' rights by participating in that program. [12]

- Amazon.com's Alexa Internet subsidiary said Friday it will pay up to $1.9 million to its customers to settle a class-action lawsuit. At least five different suits were filed against Alexa and Amazon, beginning in January 2000. The suits accuse Alexa of sending confidential information about Alexa users to Amazon without their consent. [13]

From these cases, we can infer that company, though companies have legions of personal information, are not willing to abuse them. Because they have to take the punishment of data abusion into consideration when they want to illegally distribute data. As long as the punishment is huge, companies would not take a venture for data abusion.

2.5 Technology Development

Some people threats public that the development of techonology would steal all your privacy on the Internet, leave no place for you to hide. They argue that the quickly emmergence of e-commerce would capture all your interests and stytle, database technology would remember every bits of your behavior. Powerful search engine enable others easily to identify you. Indeed technology is the main reason for the privacy violation, if the technologies are used in this way. But the question is that do technologies can use at any will? Is there restriction in front of them to avoid the misusage?

These questions remind me the time when the first clone sheep Dolly is born. After cloning was successfully demonstrated through the production of Dolly, many other large mammals have been cloned, including horses and bulls. Rumor arose when more and more exmaple of cloning successed. People who are afraid of the day of cloing human accuse that techonology would bring disearster to the world. But 12 years have passed, the people who oppose the cloning technology would even not remember what they have said. Technology is not the source of disearster of the world, people who abuse them would be the one.

As to the Internet technology, the reason for researchers and engineers improve them is to provide more useful, powerful, and convinient tools for people to better use the Internet. They would not be the reason for the privacy violation.

3. Efforts to protect privacy

Besides the ungrounded elements in the countercliam, there are several evidence that would support the position of “Privacy would not be dead, now and in future.”

3.1Intrinsic of Privacy Protection

Privacy protection is intinsical for human beings. Latanya said in [16] that we literally can't live in a society without it. Even in nature animals have to have some kind of secrecy to operate. For example, imagine a lion that sees a deer down at a lake and it can't let the deer know he's there or the deer might get a head start on him. And he doesn't want to announce to the other lions what he has found because that creates competition. There's a primal need for secrecy so we can achieve our goals.

Besides the basic need of privacy, Latanya said that privacy also allows an individual the opportunity to grow and make mistakes and really develop in a way you can't do in the absence of privacy, where there's no forgiving and everyone knows what everyone else is doing. There was a time when you could mess up on the east coast and go to the west coast and start over again. That kind of philosophy was revealed in a lot of things we did. In bankruptcy, for example. The idea was, you screwed up, but you got to start over again. With today's technology, though, you basically get a record from birth to grave and there's no forgiveness. And so as a result we need technology that will preserve our privacy.

When things turn into online enviroment, the desire for protecting provicy would never decrease. No one want to others to get their personal information without their permittion. It is uncomfortable when

you casually open a web page, noticing that your name is at the beginning of the page and the items you viewed and bought at the center of the page, at the same time you have no idea about what had happened. As the possibility and ease of tracing people and identifying people on the Internet, people need more privacy protection than ever before.

3.2 Protection from Laws and Government

Privacy involves large aspects of people, company and various kinds of organization. As privacy violation can not be quantitilized, for example, you feel violation on your privacy when you find your information unexpected appearing in a website, it is hard of you to articulate how many or how much you feel be violated. It is also not easy for people to authenticate privacy violation. We need laws and regulation to support the measurement of privacy, the right to protect privacy. Fortunately, there are many cases of existing law for privacy pretection. For example, the European Union's Privacy Directive, Council Directive 95/46 of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, (or EU data protection law), is probably the most comprehensive attempt to protect informational privacy, although experts disagree about its domestic and especially extraterritorial effects. [2]

3.3 Protection from Technology

Everythings has two sides including technology. Above we have discussed several kinds of technologies that would violate customer privacy and worsen the enviornment of online privacy. In this section, we discussed several technologies that would be useful for privacy protection.

- Privacy Enhancing Technologies (PET) attempt to achieve anonymity by providing unlinkability between an individual and any of their personal data.

- Technologies for anonymising the transport medium aim at hiding the original identity of the consumer in a way that his identity cannot be revealed. One of the simplest possible ways to achieve this for a user is to simply set up an account with a free email service provider the user trusts that they will not log communication details.

- A further step in technical complexity is a setting without a trusted third-party

- Related to anonymous access is the use of an authentication and authorisation infrastructure (AAI). CA eg.

- using statistical database: A statistical database is a data collection, for example all customers and their items bought but not revealing information that uniquely identifies the individuals.

- using privacy preserving protocol: https, kerberos. (I come out with this)

- P3P is a standard intended to enhance consumer privacy protection. It is being developed by the World Wide Web Consortium (W3C). P3P-enabled sites will include machine-readable information indicating the data the site collects and how the data will be used. Users will enter their privacy protection preferences in their browser, which will display a warning if no privacy policy is displayed or the site is gathering data the user does not wish to disclose. The next release of Microsoft's Internet Explorer will incorporate P3P technology[14] [15].

4. Conclusion

Privacy is not dead especially when more and more attention put on this issue. When people don’t unconcern about their personal data available on the Internet, when government and legislation work together to set laws and regulation to support people pursuing the right of privacy protection, when technologies towards privacy protection are used more and more in our daily on-line transaction, it is sure that the future for privacy protection would be promising.

Though it is true that customers sometimes trade their important personal information for some benefit provided by online service provider, companies would abuse customer data for malicious goals, and technology would to some extent help the violation of privacy, but this do not determine that privacy would be dead. With the effort mentioned above, we can be confident about the future of our privacy online.

We must admit that limited amount of privacy disclosure would benefit a lot to the customers. There would be balance for usability and privacy protection in the software. As a web service developer, they must decide on the extent to collect

customers information, use carefully for the intent of usability under the consideration of current laws and regulations.

There are several things we could do in future based on this basic research on privacy in the Internet. First, we can conduct research in existed privacy software for improvement and enhancement. Secondly, we can consider the content of policy that would useful for privacy protection. Thirdly, we can study several cases of existed privacy-oriented software to figure out the tradeoff between privacy protection and service usability.

Acknowledgements

Thanks to the Rebecca Wright for her valuable suggestion of finding related research material and suggestions on this paper.

Reference

[1] Amazon http://www.amazon.com

[2]http://europa.eu.int/comm/internal_market/en/media/dataprot /law/index.html

[3]Simson Garfinkel, Database Nation: the Death of Privacy in the 21st Century, Oreilly, Jan. 2000

[4]Brock N. Meeks, Invasion of privacy Dec.8 2000

[5]Mark S. Ackerman, Lorrie Faith Cranor, Joseph Reagle, "Privacy in E-Commerce: Examing User Scenarios and Privacy Preferences", E-COMMERCE 99, Denver, Colorado, 1999

[6]Ecommerce Journal http://www.ecommerce-journal.com/forum?c=showthread&ThreadID=545&page=1

[7]Consumer Privacy: http://www.faqs.org/docs/ecom/privacytext.html

[8]Nike, http://www.nike.com

[9]Lenovo, http://www.lenovo.com

[10]John Borland, "Wireless Phone Tracking Plans Raise Privacy Hackles", CNET, Nov. 10, 2000, available at http://news.cnet.com/news/0-1004-200 -3624256.html?tag=st.ne.ni.gartnercomm.ni

[11]Ponnurangam Kumaraguru, Lorrie Faith Cranor, "Privacy Indexes: A survey of Westin's Studies", CMU-ISRI-5-138, Dec. 2005

[12]Who Owns Customer Data? http://www.ecommercetimes.com/story/51347.html

[13]Amazon unit settles privacy lawsuit http://news.cnet.com/Amazon-unit-settles-privacy-lawsuit/2100-1017_3-256663.html

[14]John Schwartz, The Nexus of Privacy and Security, NEW YORK TIMES, Dec. 8, 2000, available at http://www.nytimes.com/2000/12/08/technology/08SECU.html.

[15]World Wide Web Consortium, P3P Public Overview at http://www.w3.org/P3P/Overview.html

[16]Latanya Sweeney, http://www.sciam.com/article.cfm?id=privacy-isnt-dead&sc=WR_20070710

[17]Sokratis K. Katsikasl, Javier Lopez and Gunther Pernul3, "Trust, Privacy and Security in E-Business: Requirements and Solutions Advance in Informatics",2005, pp:548-558.