Richmond Journal of Law and Technology

Volume 7 | Issue 2 Article 6

2000

Consumer Privacy on the Internet

Andrew Shen

Follow this and additional works at: http://scholarship.richmond.edu/jolt

 Part of the Consumer Protection Law Commons, Internet Law Commons, and the Privacy Law Commons

Recommended Citation

Andrew Shen, *Consumer Privacy on the Internet*, 7 Rich. J.L. & Tech 11 (2000).
Available at: http://scholarship.richmond.edu/jolt/vol7/iss2/6

This Symposium Information is brought to you for free and open access by UR Scholarship Repository. It has been accepted for inclusion in Richmond Journal of Law and Technology by an authorized administrator of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.

The Richmond Journal of Law and Technology

Volume VII, Issue 2,

Fall 2000

Consumer Privacy on the Internet

by Andrew Shen(*)

Cite As: Andrew Shen, *Consumer Privacy on the Internet*, 7 RICH. J.L. & TECH. 11 (Symposium 2000), *at* http://www.richmond.edu/jolt/v7i2/shen.html.

[The first portion of this presentation was lost due to technical difficulties]

{1}If we do not bear the loss of this privacy then the prices would be passed along to consumers anyway. We're between a rock and a hard place there's nowhere that we can go. But I think we can be more optimistic than that and I think we can preserve privacy and I think we can further growth of electronic commerce. So let me begin with the consumer perspective. I would like to start with a trend that Mike has already done a good job of starting us out on, and that is the current popularity of personalization and customization. And this is the idea that when you go to the site they will know who you are so that they will be better able to serve you. Last year Jeff Bezos was was named Time Man of the Year for his contributions in Amazon's leading role in e-tailing world. But the most interesting part about his interview, his article in Time magazine, was towards the end when he described what Amazon wanted to do for consumers. He described that Amazon was trying to was to create a nirvana experience. That is, you would go to Amazon.com and they would give you the product you've been looking for all of your life but you didn't even know you wanted. I don't know how you all feel about shopping for others, but I was completely lost about what to get my mom for Christmas last shopping season, I'm surprised that Jeff Bezos will know.

{2}So where does all that data come from? A lot of it comes from transaction generated data or what is called click-stream data. It's all about where you're clicking on a website. The links are following the products you are looking at, the descriptions for, and what kind of searches you are conducting. It takes it to an extremely minute level: how long you are pausing on a page? How long you're taking to read a description? Which areas of their website you're looking at? If there's a box on the left do people tend to click on the left as opposed to the bottom right corner of the screen? So the amounts into detail to which the data can be collected is almost unlimited. But I think the borderline between what is permissible personalization, what is an invasion of privacy to some, and what is a convenience to others is the role of the consumer in this interaction and whether the role of the consumer is an active or passive one. An active customization is where

the consumer is allowed to control what he sees. If any of you have ever gone to the Yahoo! site, there's a button at the top that says My Yahoo! and you can customize your own page. Some people like that page at one page to go to where you can check your stock quotes, check travel deals, check sports scores, news headlines, and things like that. Things that you want to see that you get to choose to have presented to you. There's also a growing amount of information collected through passive participation of the consumer. That is the consumer does not know that anyone is collecting the information. But the general rule is that if you are doing anything on the Internet it is probably being recorded. I think very little of the collection gives the consumer a very active role in that process. An example of passive information collection is the company Double-Click. Double-Click is an Internet advertiser, the world's largest with an amazing market valuation, amazing revenue, amazing resources. Basically all they do is present banner advertisements. Banner advertisements are the little boxes at the top of very popular high traffic sites, such as portals, and what they do is give you information about deals, what's going on, an ad for a trip to Hawaii. If you click on the add it will take you to the Travelocity site you will be presented with the terms of the deal for example, but also what Double-Click does is to target its ads. Double-Click actually presents on Yahoo! But also thousands of other sites,sites encompassing portals encompassing e-commerce sites, encompassing very popular news sites, such as Washingtonpost.com. So what they do is that they collect information on what you are doing on all these sites so that they can tailor their banner ads in Jeff Bezos like fashion. When made aware to the public exactly what Double-Click was doing, a lot of people opposed it. Beginning this year that focused a lot of attention that company and their plans - to collect a lot of profile information and also to link that information with personal data including your name and mailing address and that received a lot of opposition . The ability to link that day was through a common technology called cookies. Something I get asked about a lot is what exactly is a cookie? I think people want a very concrete explanation. The cookie is a small text file placed on your computer by the website server. It resides on your computer and is sent back every time you return to that site. You can think of it in terms of an ID badge. This ID tag is passed from your computer every time you go back to that site, so if I go to Yahoo!, Yahoo! will know it's me. If I see a Double-Click banner ad, Double-Click will know it's me. Information is constantly being passed back and forth. Most consumer don't know about this because many of the default settings on many popular browsers such as Internet Explorer and Netscape Navigator allow cookies to be passed back and forth indiscriminately. Although people don't know what cookies can do and how to control them, there are ways to do that, we will talk about that later.

{3}What sort of limits are there now? I don't want to give you the illusion that there are none. There are a few. The Federal Trade Commission has jurisdiction over commercial websites and their activities with respect to privacy. Their enforcement usually comes from the enforcement of privacy policies. One of the major problems with privacy policies is they are very confusing to the average person. And people who don't understand what cookie technology is and who don't understand what click stream data is. Where the FTC comes in is that it can enforce these policies under what is called Deceptive or Unfair business practices. If the company's site were being deceptive, the FTC can take action. If the website is being unfair in the terms of its interaction with consumers the FTC can also take action. I think there are also limits that give you a couple of examples and I'm going to read you a quote from Toysmart.com's privacy policy from just a couple of months ago."At Toysmart.com, we take great pride in our relationships with our customers and pledge to maintain your privacy while visiting our site. Personal information voluntarily submitted by visitors to our site such as name, address, billing information and shopping preferences is never shared with third party." That turned out to be a deceptive statement which the FTC did pick up on because Toysmart, just a couple of months ago actually tried to sell all of its personal information. The FTC settlement in that case was far more controversial. The FTC created a few limits and requirements that the company warned to purchase those lists would have to meet. Nonetheless toysmart will likely be able to sell this information in the future. Interestingly, what if Toysmart had said from the very beginning,"right now we are taking very good care of your information but in the future we will not. And if the opportunity presents itself we will sell it." That would be perfectly legal under the Federal Trade commission's current jurisdiction and current authority. And I would like to give you one more example; this is from the current Amazon.com privacy notice. That

company recently changed its privacy policy. It currently says: "Our business changes constantly. [very considerate of them to tell us that] This notice and the conditions of use will change also. And use of the information we collect is subject to the privacy notice in effect at the time of use." I think that would constitute an unfair business practice. For example if I am a consumer, and I had gone to the Amazon.com privacy notice and read all through the terms, tried to make heads and tails so what that they were trying to do with my personal data. They could change the terms of the privacy policy and their guarantees to me with respect to the data at any time with respect to the data under this privacy policy.

{4}So there are certain ways in which unfair and deceptive business practices can come in and can influence what a company can do with personal data but I think the important thing to point out is that the FTC's authority comes through deception and unfairness. But there are truly no privacy standards. Companies do not acquire your consent before collecting personal data. Companies do not have to let you see the information that they have already collected about you. Companies don't have to ensure the security of that data and so on and so. Those sorts of privacy standards and limits that a company would have to follow are not there.

{5}There are a couple things we can do. First, I would like to talk about a group of tools called privacy enhancing technologies which in some ways brought us into the situation, and technology can help us get out of it. Privacy enhancing technologies promote anonymity. That is they limit the amount of personal information disclosed in a normal transaction. You can think of them in different ways. You can have anonymous communication; it is currently possible to send a completely anonymous e-mail to someone around the world and they will have no idea who it is and no way to trace it back. Anonymity in payment; as an off-line example, you can think of the European telephone cards or the Metro cards in DC. You pay for everything and they will never know who you are. There is anonymous Internet surfing. Various products are out using very fancy technology that I don't completely understand such as proxy servers, encryption, onion level routing (basically ensures that your mutation with a website can't be traced back to you are). So obviously there's a lot of information out there that can help us; they can help us protect our anonymity. But there's also false privacy enhancing technology and I would like to spend a couple of minutes talking about that. Just because there's something that helps you with your personal data and has all sorts of computer tools and computer manuals and technical stuff behind it does not mean it's always going to help you protect your privacy. A good example of that is the growing industry of infomediaries. Infomediaries will keep your information on file. You give them an entire description of who you are, what you do, and what your tastes are and what you are interested in and they will disclose that information to the website you're actually communicating with. Another one of these false privacy enhancing technologies is one called P3P, or the platform for privacy preferences. Similar to infomediaries they will not necessarily limit the amount of information you are disclosing. In many cases, they may help you disclose more information since you have entered it somewhere and can send it off with the click of a button.

{6}So what is the answer? We're trying to deny the undeniable in some people's eyes. We are trying to stop invasions of privacy where they are right now and maybe you can get some of them back. I think the answer is twofold. One is that we clearly need a legal standard for privacy protection. The FTC act is very limited in its legal authority to establish standards for what is done with your personal data. Fair information practices have to be a core component of the legal standard. In the FTC's eyes, fair information practices includes things such as notice - provided with a privacy policy, you can see what's going on, access, choice - you have someplace, somehow the ability to keep your information from being collected, and security. But I think a fuller range of fair information practices will include other principles which are very important. Principles such as purpose specification - just because a company asks for your permission does not mean they can use it for anything they wish. They should only be able to collect data for specific purposes in specific instances. There should be a limited use, this information collected for one thing should not be used for another. If I give my mailing address to Amazon for a book, they can sell that information to a database marketer so I get junk mail. Of course I think the ability to challenge the compliance of many of these companies. Right now

consumers are not aware of any rights of their own to challenge these companies for what they think are invasions of privacy. Right now the Federal Trade Commission does act from time to time on individual complaints that there is no procedure for individuals to pursue actions to pursue companies without the involvement of the FTC. I think once we establish the legal standard that will encourage good business practices. Currently, a lot of companies are collecting a lot of personal information and the attitude of many of the companies is "if he can do it, I can do it too." There's a race basically for as much information as possible. But I think a legal standard will eliminate some of the more invasive practices. And as I said before we need to, in addition to the legal standards make use of the technology available; ones that will limit the dissemination of personal information and ones that will promote anonymity. And for those of you interested in business I recommend that people who look at e-commerce businesses think about privacy from the very beginning. Obviously the Internet is a place, a sector where privacy is a very important issue. I've seen numerous polls saying that is a major concern. A simple saying that people are more concerned about privacy than about credit card numbers being intercepted over website. I think there are the obviously caveats when you cite polls statistics but I think after you start seeing a number of these polls you start to wonder. I think e-commerce businesses should think about how to build in privacy and to use personal data from the very beginning, because I think you have seen a backlash against these companies that forced to changing in behavior but at some cost of their operations. I hope that helped you to think about privacy a little bit and don't be so pessimistic about it in the future.

---

[*] Andrew Shen is a policy analyst at the Electronic Privacy Information Center (EPIC). EPIC is a public research center based in Washington, D.C., that works on emerging cyber-liberties issues. Andrew primarily works on issues relating to information privacy -- the rules surrounding the collection and use of personal data. He has served as a panelist at the Federal Trade Commission (FIFC) Workshop on Online Profiling and as a member of the FI'C Advisory Committee on Online Access and Security.

Mr. Shen has previously worked with the American Civil Liberties Union (ACLU) and is a graduate of Stanford University.

Return to this Issue's Index

Return to *The Journal's* Home Page

© Copyright 2000 Richmond Journal of Law & Technology