December 2001

Internet Privacy: At Home and at Work

Robert Boncella
Washburn University

INTERNET PRIVACY: AT HOME AND AT WORK

Robert J. Boncella
Washburn University
zzbonc@washburn.edu

Abstract

This paper is a summary of the tutorial on Internet privacy. The objective of the tutorial is to inform users of the Internet how and why their use of the Internet can be monitored. The focus of the tutorial will be Internet privacy at home and in the work place. The tutorial has three major sections: Technical Background, At Home and At Work.

The At Home section is concerned with personal privacy infringement. This section will detail who would be interested in personal privacy infringement, how they would accomplish it, and for what purpose. This portion presents topics such as cookies and their uses and log files. In addition the At Home section discusses techniques to avoid privacy infringement (e.g. anonymizers, cookie cutter).

The At Work section is concerned with employee surveillance. The topics discussed include who would be interested in this surveillance, how this surveillance would be done and for what purpose. The At Work section also discusses the concept of Acceptable Use Policies (AUP). Questions address: What purpose do AUP serve? How do AUP support or detract from employee surveillance? Both sections require a bit of technical expertise to understand how Internet activity can be monitored. The Technical Background section reviews the client/server paradigm of web computing, the important details of the Hypertext Transfer Protocol (HTTP), and presents an overview of Uniform Resource Locators (URLs). These concepts are necessary to understand how Internet activity con be monitored.

Keywords: Internet privacy, acceptable use policy, cookies, web bugs

Introduction

In the confines of your office, study or cubicle the Web feels anonymous - IT IS NOT. Everything that one does on the Web can be monitored automatically. Why monitor? When we discuss privacy at home your personal information and web habits can be useful for marketing purposes. While at work, knowing an employee's web behavior can be useful in determining an employee's productivity.

Technical Background

Three fundamental concepts allow the World Wide Web to be an efficient and effective means to deliver information. These are: the client/server method of computing (sometimes called the request/response paradigm); HTTP (Hypertext Transfer Protocol); and the URL (Uniform Resource Locator) syntax/semantic. The request/response paradigm is used to implement the web browser – web server interaction. HTTP is used to coordinate and control this interaction. And URLs are used to identity an information resource uniquely on the Web. When a user – through a web browser - requests a web page from a web server these three concepts combine in such a way that the information of who is requesting what from where can be automatically monitored and collected. In addition if a user provides personal information (e.g. name, SSN, phone number) that information may be both monitored and collected.

Internet Privacy At Home

Private Information: Who Wants It

The forgoing description might cause concern for the user. However Web merchants, Web page advertisers, and market researchers would find it useful to know what Web sites users visit, what pages they download, and what pages they view next. These parties, e.g. DoubleClick (www.doubleclick.net), 24/7 Media (www.247media.com), and Engage (www.engage.com), are interested in users ' "click streams". They can use this information to "target" the consumer using the Web. This information is collected using several techniques. These are web server log files; cookies, and web bugs.

Private Information: How They Get It

Web server logs can collect the information from the "referer " header field in the HTTP request protocol. This information indicates the URL of the resource being requested and the URL that referred the client (user) to the requested resource.

The use of Cookies is a technique designed to overcome the "statelessness" of the HTTP protocol. When a web browser requests a resource from a web server it establishes an Internet connection with that sever. Once the server sends the response to the browser's request that connection is terminated. If the same web browser makes a request to the same web server at later time that web server has no information regarding that browser's last request – the web server does not remember the state of that web browser. This is a difficulty when the user is shopping on a web site and filling a shopping cart with items from different pages. To enable the server to remember the state of a browser (e.g. what items are in its shopping cart) the server sends a cookie to the browser when the browser make its first request to that server. The browser then returns the cookie to the server whenever it requests another resource or service from that server. A cookie can be thought of as a unique ID associated with that browser and this ID can be used to located a data record stored on that server that may contain current and historical information about the web browser.

Given the HTTP protocol and how download web pages are rendered, a third party can exploit the cookie technology in order to track any user's click steam during a session. This is the idea of "web bug". Very briefly – once a browser accepts a cookie from a server that allows web bugs it also accepts a cookie from the server that serves out this web bug – call this the web bug cookie. The effect occurs every time the browser requests a resource from a server that allows the web bug the browser will return the web bug cookie to the server that serves web bugs. Ultimately a user's click stream can be monitored across web servers.

Private Information: How They Can Be Prevented

To prevent or at least manage this information collection, the user can use anonymizing proxy servers and cookie cutters.

Anonymizing proxy servers essentially carry out the request on behalf of the browser. The information sent to the web server is information about the proxy server not about the requesting browser.

Cookie cutters allow the user to determine if they what to accept a cookie from a specific server. Current versions web browsers have these features as part of their implementation

Internet Privacy At Work

The topic of Internet privacy at work focuses on employee surveillance. An organization engages in the surveillance of how their employees use the Web and their e-mail for three main reasons. These are: employee productivity; wasted bandwidth; and legal liability.

Why Corporations Conduct Web Surveillance

It has been estimated that US corporations lose more than $54 billion a year because of non-work related employee use of the web. In addition to productivity loss, bandwidth is reduced when employees use the web for non-work related activities. Finally legal liability can occur when employees improperly use web resources ranging from copyright infringement (e.g. downloading and installing software) to sexual harassment issues associated with pornographic content and inappropriate e-mail.

How Corporations Conduct Web Surveillance

Employees of medium to large size corporations will be using Internet access devices attached to a corporate network. This arrangement implies the employee must access the Internet through a proxy server managed by the organization. This arrangement makes it a simple matter both to restrict and to monitor an employee's use of the web. A number of software tools will limit access to specified web resources and can collected data on a user's "click steam". These tools are installed and managed on a proxy server.

Smaller size organizations where employee access is not managed through a proxy sever an employee's web use can be monitored by viewing the local data files associated with the user's web browser. For example, in Netscape Navigator the cache file, history file, contents of the location bar and cookies file; or the inbox, sent, trash, and drafts file of Netscape Messenger.

How Can An Employee Manage Corporation Web Surveillance

Employees will not be able to manage corporate web surveillance but they should be made aware of it. Specifically, employees should know the Acceptable Use Policy (AUP) for computing resources if one is provide by the organization. Part of that AUP should be a specification of the organization's Internet Access Policy (IAP). If no AUP is provided to an employee then the employee should request the AUP. If the organization does not have an AUP in place then a process should started to develop an AUP for the organization.

Summary

In the confines of your office, study or cubicle the Web feels anonymous - IT IS NOT. Everything that you do on the Web can be monitored automatically. If you use the web then you need to be aware of the how and why this activity can be monitored.

References

Angel, Jonathan (2000) "Too Many Cookies Are Bad for You", *Network Magazine*, (15)6, pp.106-112.

Benassi, Paola (1999) "TRUSTe: An Online Privacy Seal Program", Communications of the ACM, (42)2, pp.56-59.

Clark, Elizabeth (2000) "Privacy on the Internet", *Network Magazine*, (15)6, pp.99-100.

Clarke, Roger (1999) "Internet Privacy Concerns Confirm the Case for Intervention", Communications of the ACM, (42)2, pp. 60-67.

Conry-Murray, Andrew (2001) "The Pros and Cons of Employee Surveillance", *Network Magazine*, (12)2, pp. 62-66.

Cranor, Lorrie Faith (1999) "Internet Privacy", Communications of the ACM, (42)2, pp. 29-31.

Dalton, Curt E, (2001) "Preventing Corporate Network Abuse Gets Personal", *Network Magazine*, (12)2, pp. 56-60.

Davis, Tony and Royce, Doug (2001) "The Law of the LAN: Monitoring Employees' Electronic Communications", *Network Magazine*, (12)2, pp. 50-54.

Dornan, Andy (2000) "Internet Indiscretions", *Network Magazine*, (15)6, pp.100-105.

Garfinkel, S. and Spafford, G. *Web Security & Commerce*, O'Reilly and Associates, Cambridge, MA, 1997.

Goldschlag, David, Reed, Michael, and Syerson, Paul (1999) "Onion Routing for Anonymous and Private Internet Connections", Communications of the ACM, (42)2, pp. 39-47.

Mulligan, Deirdre and Schwartz, Ari (2000) "Your Place or Mine?: Privacy Concerns and Solutions for Server and Client-Side Storage of Personal Information", *Proceedings of the Tenth Conference on Computers, Freedom, and Privacy: Challenging the Assumptions April 4-7, 2000 Toronto, ON Canada*, pp. 81-84.

Reagle, Joseph and Cranor Lorrie Faith (1999) "The Platform for Privacy Preferences", Communications of the ACM, (42)2, pp. 48-55.

Reiter, Michael and Rubin, Aviel D. (1999) "Anonymous Web Transactions with Crowds", Communications of the ACM, (42)2, pp. 32-38.

Stein, Lincoln D., *Web Security: A Step-by-step Reference Guide*, Addison-Wesley, Reading, MA, 1998.

Treese, Win (2000) "Data Collection and Consumer Privacy", *Networker*, December 2000, pp. 9-11

W3C, (2001) "P3P 1.0: A New Standard in Online Privacy", http://www.w3.org/P3P/brochure.html

Wadlow, Thomas A. , *The Process of Network Security: Designing and Managing a Safe Network*, Addison-Wesley, Reading, MA, 2000.