Chapter 15
Who Is Tracking You?
A Rhetorical Framework for Evaluating Surveillance and Privacy Practices

Estee Beck
The University of Texas at Arlington, USA

ABSTRACT

Exchanging information online often involves a degree of assessing the credibility and reliability of websites, which include the authors, sources, and content. This chapter argues for an additional assessment category: evaluating privacy and/or data use statements of websites because of the underlying ideologies, methods of tracking technologies used to collect data, and the need for comprehension of what website terms and conditions mean for the average person. This chapter provides a rhetorical framework as suggested guidelines to follow when evaluating privacy and/or data use statements of websites.

INTRODUCTION

As Adrienne Lafrance (2015) noted, the average lifespan of a webpage is only 100 days; however, as of late 2015, there are over 1 billion webpages in existence (Internet Live Stats, 2016). With the volume of webpages in existence, there is often a need to assess the credibility and reliability of websites in order to establish the validity of the information contained therein. To help with such an endeavor, the International Federation of Library Associations has provided research on methods for evaluating sources as part of a larger literacy and reading integration matrix (Farmer & Stricevic, 2011). Concurrently, the American Library Association has devoted space for an online lesson plan database providing professionals with curriculum materials—including lesson plans on evaluating websites (Lomanno, n.d., Ricker, n.d., Steinhauser, n.d.). Even the Reference and User Services Association, a Division of the American Library Association (2015), has a dedicated site for finding, evaluating, and using primary resources on the web. Much of the literature and professional reports result from the need to teach students how to evaluate websites in an age where anyone can launch a webpage with unreliable and untrustworthy information. Studies from the mid-2000s reveal many students do not critically evaluate website content (Killi, Laurinen, & Marttunen, 2008; Kuiper, Volman, & Terwel, 2005; New Literacies Research Team & Internet Reading Research Group, 2006).

DOI: 10.4018/978-1-5225-7113-1.ch015

The research on evaluating the credibility of websites suggests evaluation metrics under categories such as author affiliation and authority, evidence of authenticity or bias; currency or recency; and website content. While these areas provide a strong foundation for evaluating website credibility, an often overlooked area is analyzing websites based on surveillance tracking technologies alongside website privacy policy statements. This is potentially problematic given the often complex ideologies governing policies and procedures of websites, not to mention the sophisticated methods for collecting, storing, and profiting from the data of its customers or users employed by many websites such as Google, Facebook, Amazon, Netflix, and Dictionary.com use (Beck, 2015). Tracking cookies—small alphanumeric files used to track browsing histories—are part of a refined approach to collecting intimate data on individuals. Many websites use tracking cookies; however, in many cases it is less clear how the websites use the data—whether it is for internal purposes or for profit. Existing research in this area indicates there is reason to apply caution before consenting to the terms and conditions of websites because businesses more often use data to identify, track, and intervene on private citizen's lives without real cause (Hoback, 2013; Degli Esposti, 2014).

In light of the complex mechanisms governing website terms and conditions, tracking technologies, and website policies, this chapter seeks the inclusion of a rhetorical framework—a set of guiding heuristics grounded in the rhetorical tradition—for evaluating website surveillance and privacy practices in order to explore how one might come to view information—and accurately assess—the credibility and reliability of websites from a privacy and security perspective. Since evaluating sources is not a new concept to critical thinking or the research process, my discussion herein focuses on surveillance culture generally, with a deepened emphasis upon evaluating website credibility through surveillance techniques and privacy policy statements. Digital surveillance and privacy play an integral role in networked communication. Making decisions about *which sites* get *what data* from website customers/users is part of developing a digital literacy skillset. This chapter provides background for the importance of this evaluation area, and then moves to contemporary scholarship and news media sources addressing surveillance and privacy issues online, ending with strategies for developing a rhetorical framework based upon localized and individual needs.

BACKGROUND

Although most websites have some type of data and/or privacy policy statement disclosing how the site collects, uses, and discloses user data, it can be difficult to understand the legal protections offered to people. In the United States, for example, there are no federal privacy laws mandating that companies issue data/or privacy policy statements—or any type of industry or legal consortium offering common guidelines for developing statements for website users to understand with ease. However, there are three U.S. federal acts giving provisions to website operators for areas of finances, health, and the protection of children[1] under the age of 13. Yet, these three laws are written for the protection of companies with websites in the United States against privacy lawsuits. On the other hand, the European Union adopted a directive in 1995, the Data Protection Directive (Directive 95/46/EC) that provides a data protection system for privacy within and across EU borders for individuals. Additionally, this directive has had a direct impact on American industry seeking to do business in the EU with ramifications felt in interna-