The Invisible Digital Identity: Assemblages in Digital Networks

Estee N. Beck
Bowling Green State University

Abstract

Using tracking cookies and web beacons, online behavioral advertising uses code stored on machines to access users’ Internet habits to customize advertisements and better market goods to consumers. This trend of tracking user movements has become concerning because the technologies used reveal personal information about the user to companies. Users can become more informed about the tracking technologies by visiting two websites that provide information about the trackers and give ways to opt-out of tracking technologies. This article provides a historical overview of tracking technologies, analyzes AboutAds.info and the online privacy tool Ghostery <ghostery.com>, theorizes what networked culture means in the 21st century, and closes with a heuristic for educators to use in their classrooms for discussions about invisible digital identity on the web.

© 2015 Elsevier Inc. All rights reserved.

Keywords: Digital identity; Surveillance; Cookies; Web beacons; Online behavioral advertising; Object-oriented rhetoric

Strategically hidden inside our computers are files that track our movements on the web. Inside the files are long strings of alphanumeric codes that do not reveal, on the surface, the kinds of personal information they contain. Concealed inside the code, such personal data includes housing type, age, sex, income, spending habits, hobbies and interests, items bought, items you’re interested in buying, if you’re traveling soon, and other data that may be fairly revealing. We live in an age of invisible digital identities where companies track our demographic information, habits, and online behaviors, and in some cases, sell this information to third-party companies for profit.

Interested in what my invisible digital identity consisted of and what tracking technologies had gathered about my online identity, I turned to BlueKai, a “big data” activation company that brands data for marketing purposes.

1 I would like to thank Kristine Blair for reading through earlier versions of this manuscript and providing encouragement, feedback, and insight. Additionally, I thank the blind reviewers for their gracious feedback and direction. Lastly, I thank Matthew Bridgewater, Mariana Grohowski, and Megan Adams for reading through a much earlier version of this manuscript and providing helpful directions.

E-mail address: enbeck@bsgsu.edu

1 Estee N. Beck is a PhD Candidate in the Rhetoric & Writing program, Department of English, at Bowling Green State University. Her current research positions computer algorithms as persuasive agents capable of shaping and influencing writers in digital spaces. She regularly tweets from @este Beck.

2 It is important to note here that there are several definitions of big data that are highly dependent upon the field or organizations’ purposes. According to Thomas H. Davenport, Paul Barth, and Randy Bean (2012), data scientists can capture big data from an array of sources, including “clickstream data from the web, social media content (tweets, blogs, Facebook wall postings, etc.) and video data from retail and other settings and from video entertainment. . . . [it] also encompasses everything from call center voice data to genomic and proteomic data from biological research and medicine” (p. 43). Big data is a conglomeration of virtual human behavior that involves some form of digital technology that computers and people have the ability to track and analyze. Big data is also pay dirt for organizations who seek advantages over competitors to capture consumer interest and money, especially through custom advertisements based on demographics and online behaviors.

http://dx.doi.org/10.1016/j.compcom.2015.01.005
8755-4615 © 2015 Elsevier Inc. All rights reserved.
Within their website, an option reveals consumers’ invisible digital identities by threading files from various tracking technologies and illustrates how companies brand customers for customized web experiences.

The BlueKai Registry provided me with telling data about my surfing habits. It correctly identified the type of housing I live in (an apartment), my age range, sex, income level, spending habits, that I contribute to charities, that I will travel in greater than 21 days, the vehicle price-range of my car, and that I may want to buy concert tickets in the near future. Granted, the data provided on the site masked more identifiable characteristics like my name or housing address; however, the data diagrammed enough about my surfing habits to place me in certain behavioral categories, which allowed for the type of segmentation marketing companies create to motivate me to click an advertisement. All of this information came from the various tracking technologies embedded within the Firefox browser I used.

As digital rhetoricians and digital writing instructors, we have been concerned with digital identity representation, and rightly so, because we’ve focused our efforts on the types of data elements we can control, like developing virtual professional identities and showing our students how to cultivate a healthy online presence. We have, in turn, come to see our visible digital identity as something we can somewhat regulate online. On the other hand, with each click of a web page, we also have an invisible digital identity constructed through third-party elements and tracking Technologies. I find this concerning, as with each click, fragments of our interests, habits, and demographics are stored, collected, and—in some cases—sold. In the Web 2.0 and Web 3.0 eras, our invisible digital identity—constructed through our consent of using web pages—is for sale. This trend of collecting and distributing fragments of our digital identity has led me to think about the ways digital writing teachers ask students to get online, click around, and use certain websites for course projects. Additionally, I wonder how we might better inform our students and each other about the types of online writing environments they and we engage with on a daily basis. Hence, my goal here is to share information about how our invisible digital identities develop through third-party elements and sites that track these elements to foster awareness among digital teachers and researchers. It is my hope that through this material, educators can turn to teaching their students about the hidden files stored on their personal machines, how companies use their personal data for online behavior advertising, and what actions students can take to limit the farming of computer files of their surfing habits. This article argues that if educators ask students to dig into digital spaces that use tracking technologies, then they also have some responsibility to teach students about invisible digital identities, how to become more informed about digital tracking, and how to possibly opt-out of behavioral marketing.

After all, discussions about visible digital identity and privacy are important to have with students. Scholarly essays and chapters have provided digital researchers and teachers with a rich understanding of identity online connected with social identity (Blackmon, 2003), developing digital identity with young women (Blair, Dietel-McLaughlin, & Graupner-Hurley, 2010), sexual orientation associated with gaming and literacy (Alexander with McCoy, & Velez, 2007), and the limitations of templates driven by social media sites (Arola, 2010), but there are other issues at stake. Talking about data collection and mining, digital and online surveillance, and various tracking technologies gives teachers points to consider not only when designing a course using the web, but also when asking students to participate in spaces that track their movements and collect user data. Accordingly, Jessica Reyman (2013) argued that we need to educate not only our students, but also our colleagues and ourselves about how data information operates online and how power differentials affect our digital spaces. Altogether, there are several issues at play with web use including visible digital identities, but instructors also might turn their attention to the invisible identities all web users have and what those in turn might mean for digital writing instruction.

Considering that more people are on the Internet and using mobile technologies, we need further research into surveillance and privacy along with the specific types of information tracking technologies collect about users. According to a Nielson (2012) report on social media use, there were 204 million people connected to the Internet in the U.S. in July 2012 along with over 95 million connected through mobile technologies; while the top social networking sites are Facebook and Twitter, sites like WordPress and Wikia lead the top list in terms of engagement. With this many people connected and with more wired classrooms, there is an obligation to discuss with our students not only the kinds of digital identity and privacy that are somewhat controllable, but also the hundreds of companies that use tracking technologies to capture data to better advertise products and how that shapes interactions on the web. In short, digital surveillance matters. As digital writing instructors, we need to understand how companies use this data, especially when, in the most egregious of cases, large data points reveal inaccurate information about people that in turn affect their legal, medical, and financial lives—which has been a case with American Express negatively adjusting credit
limits based on data file collection\(^3\). These files construct a rich portrait of a digital identity that we cannot control without the help of sites that uncover tracking technologies on web browsers. Accordingly, there is a need to educate our students, as in the words of Cynthia Selfe (1999), to pay attention to how companies track our movements online and how we may opt-out and be better informed about these practices.

In this article, I provide background information on the stages of Internet development and surveillance tactics used by companies that capture information about users through their web browsing. This information illustrates how the web changed over the last two decades and how the transformation shapes our online writing environments. I then discuss tracking technologies and differences between first- and third-party cookies and web beacons to unveil the mechanizations of digital surveillance. I then move to examine two websites that cast tracking technologies into relief by providing evidence I collected from these sites about what tracking technologies revealed about me to prompt exploration of these sites. The next section theorizes an assemblage of digital networks using object-oriented rhetoric to conceive of what a 21st-century panoptic environment means for digital writing research. I then close with recommendations for educating students on tracking technologies, including how to frame talks about this material. I open with why this matters for digital environments and digital writing instruction.

1. Paying attention to what is happening with the Internet and digital identity

The shaping of discourse surrounding computer technology environments stresses resisting the binary between humans and technology—or technology as a tool to foster human pursuits. In his personal narrative on writing technology, James Porter (2002) asked, “How much do these computer-based writing technologies really matter in terms of their effects on writing” (p. 384)? He concluded that they matter a great deal—writing technologies, especially computer-based technologies, shaped him as a writer through a complex rhetorical, social, and cultural matrix whereby the machine and he engaged in a cyborg relationship. This shift in thinking helps scholars and researchers tease out a common binary of humans versus technologies or technologies as tools and think about the networked and relational engagements with objects through distributed networks. In particular, this concept sharpens our thoughts about immaterial objects like algorithms—how code spreads and interacts with other code thereby suggesting an object-to-object relationship independent of human interaction. This also leads us to question how algorithms and tracking technologies output data that plot decisions upon virtual and physical bodies. The pulse of online engagement influences user interaction in virtual environments—shaped by the very code nabbing bits of user data for a fluid web experience. As digital writing instructors, we manage talks with students about writing spaces and the effects environments have upon writers. Such talks mirror what Dannielle Nicole DeVoss, Elyse Eidman-Aadahl, and Troy Hicks (2010) have elsewhere put forward about digital ecologies and how humans interact and adapt to digital environments. These environmental factors include hardware and software, networks, privacy, surveillance, physical and virtual spaces, along with other legally protected and unprotected classes such as sex, gender, ethnicity, and even sexual orientation. Increasingly, we can no longer ignore tracking technologies in our digital spaces.

Focusing on one aspect of digital ecologies—cookies and web beacons—helps digital writers and researchers understand the historical growth of tracking technologies and how digital tracking technologies help companies and organizations collect large data sets. Enhancements to cookies during the early 2000s led to sophisticated online surveillance practices when companies learned users deleted cookies as fast as they were installed on machines. Advertisers also sought out ways to increase revenue by tailoring advertisements to users based on their browsing habits. While social media began its meteoric rise with budding and now non-existent or nearly non-existent sites like Friendster and MySpace, the focus on digital identity became what a user could conceivably control. However, underneath the veneer of user-controlled digital identity, major corporations and companies began ways to track users’ every movement on the web to increase revenue by either direct marketing or selling the data collected to other companies (see McKee, 2011). Thus, digital identity has several definitions—whether it is through controllable

---

\(^3\) According to Allstair Croll, big data is a “civil rights issue” because it is not the volume of data available, but the way companies use algorithms to analyze the data to make adverse decisions about people citing that “‘personalization’ is another word for discrimination” (2012, para. 12). He cites an ABC news story where American Express negatively adjusted the credit limit of a customer based upon where he shopped without taking into account the customer’s excellent FICO score based upon the justification, “Other customers who have used their card at establishments where you recently shopped have a poor repayment history with American Express” (Cuomo, Shaylor, McGuirt, & Francescani, 2003, para. 12).
information, as is the case with associating a real-life name with digital projects, or the rich portrait of online habits and behaviors assembled from tracking technologies that might suggest an identity that some people may not feel comfortable with companies having access. Additionally, digital identity takes root in Manuel Castells’ (1997/2004) notion of identity, or that which becomes internalized and constructed from social conditions by actors. I add that identity, connected with digital surveillance and tracking technologies, assumes a symbolic position of identity as constructed by computer algorithms and tracking technologies, and those data elements become a digital apparatus for digital social engineering and marketing of virtual bodies.

The invisible digital identity, on the other hand, has three defining characteristics. First, it’s regulated. Web companies can regulate behavior of people on the Internet by controlling the flow of information. The companies do this through web customization and digital surveillance tools like cookies and web beacons. Because front-end users don’t necessarily have access to their invisible digital identity—this is a type of what Lawrence Lessig (2006) calls “regulation by code”—I argue that this leaves little agency for Internet users. Second, the invisible digital identity is made up of various virtual, non-virtual, human, and non-human cultural ecologies that exist in a matrix of various temporal, spatial, physical, emotional, political, social, financial, and legal dimensions. Both ideological concerns over potential discrimination and power as well as the materials used in the hardware of the Internet are of equal concern with the invisible digital identity. And, finally, the invisible digital identity refracts the Internet. A Google search of the term “girls” can be radically different for each user because of the information harvested from user web browsers and machines. The flow of information is fundamentally altered, changed, and personalized for each user. The potential to shape what users see online and use in their work is profound.

1.1. Stages of Internet development and surveillance tactics

Since computers entered the composition classroom in the 1970s with the creation of various software programs for prewriting, invention, revision, and grammar (see Hawisher, LeBlanc, Moran, & Selfe, 1996, p. 98), instructors have seen the computer classroom move from closed systems, i.e. a lack of Internet use, to what Leah A. Lierouw (2012) called the three stages of Internet development: the relational Internet, the enclosed Internet, and the “mean world” Internet. She further explained these terms:

The relational Internet, [is] the increasingly interpersonal and personally customized character of online and mobile communication; the enclosed Internet resulting from growing technological and legal restrictions on new media devices and systems; and the “mean world” Internet, the sense of risk and exposure online that has been used to justify the expansion of increasingly invasive private and state surveillance/security regimes. (2012, p. 617)

The move from the static Web 1.0 to collaborative 2.0 environments has certainly changed the landscape of the Internet. With more users, companies have learned to capitalize on the millions of people accessing, downloading, and sharing information on the web. At the same time, with this development, there have been increasing restrictions and governmental surveillance. Users have witnessed the turn to marketing surveillance with websites installing and accessing tracking technologies on users’ hard drives with each website visit, suggesting a turn to the “mean world” Internet. However, in his examination of Internet surveillance, David Lyon (2009) suggested that those in marketing “applaud these practices” of cookie use because “[they offer] benefits to the consumer, of customized advertising, tailored to their needs” (p. 97). George Ritzer and Jurgenson (2010) reflected on this further from the perspective of the prosumer—a term to describe both production and consumption from the customer perspective—that people seem to enjoy being prosumers because there are benefits, even if their time and labor contributing to companies and organizations is unpaid. Yet, web users may not realize the amount of data they provide as prosumers on the web. With the development of leaks by Edward Snowden that revealed how the National Security Agency contracts with telephone and social media companies for user data, it has become increasingly important for people to know how governments, companies, and organizations may or may not participate in the “mean world” Internet. This is especially true when consumer data for advertising purposes is turned over to other organizations to use for other means. Incidentally, companies like 24/7 Real Media, BlueKai, Google, Microsoft Corporation, and Yahoo! Inc. use tracking technologies for what is called Online Behavioral Advertising (OBA). According to the Network Advertising Initiative (2012)—a coalition that sets responsible and ethical privacy practices—OBA “uses information collected across multiple websites that you visit to predict your preferences or infer interests and to show you ads that are more likely to be of interest
to you.” Companies target users based upon general interest categories like education, sporting, and cats, but they can also, as the BlueKai Registry revealed of my surfing habits, gather detailed information and data including the titles of movies watched on certain sites or more revealing data.

1.2. Cookie and web beacon development

Central to unveiling invisible digital identities is an understanding of the history of tracking technologies, especially if digital writing instructors incorporate discussions about invisible digital identity in their classrooms. Generally, most users are somewhat aware of terminology like “cookies” and “cache”; however, a deeper understanding of cookie and tracking technology development helps teachers understand how various online environments might operate (see Lory Hawkes, 2007, for additional information). What follows, then, is a historical account of tracking technologies. Equipped with information about the virtual objects that track users online, educators will have knowledge about the coupling of tracking technologies with user privacy, i.e. the practice of installing cookies and web beacons on machines affects the ways in which users and writers interact with virtual spaces.

Tracking technologies have been around for well over a decade. Netscape introduced the first tracking technologies dubbed “Magic Cookies” in Navigator 1.1 (Randall, 1997). This early HTTP protocol technology captured information about users when they visited websites by placing cookies on their computers’ hard drives. When user browsed between pages, the cookies sent information to the web page’s server that had been stored in the cookies. However, with alarm about the information stored and shared in a cookie, people began to delete the cookies stored on their hard drive to help ensure their personal privacy. Concerned that people were deleting cookies, United Virtualities, a New York firm, developed what is now known as a flash cookie, an undeletable cookie, in 2005. First reported by Matt Marshall (2005), these new cookies were:

newer, tougher, and they stay around a lot longer. They come with PIE or Persistent Identification Element a little-known technology that evades cookie deletion. PIE hides within a little-known corner of your computer.

And, PIE recreates itself even after a user deletes a cookie by making a backup copy. (para. 2)

Users can delete the original cookie file, but upon deletion of a flash cookie, code automatically generates to create a backup copy. That file is then stored elsewhere on the computer outside of the de facto cookie file on the computer. While Kevin Lee of Did-it.com emphasized that people have generally come to think of cookies as harmful and that most cookies are good, what is alarming about flash cookies is the lack of an expiration date (as cited in Marshall, 2005). As Janice C. Sipior, Burke T. Ward, Ruben A. Mendoza (2011) verified, “HTTP cookies expire at the end of a session. Flash cookies by default have no expiration date” (p. 4). Any attempt to clear a browser’s cache, delete cookies from files, or even clear the history of sites visited will not delete a flash cookie. The ability to track users through cookies and flash cookies has advanced with the development of the relational Internet with advertisers and marketers finding ways to track online moves. Flash cookies stick to computer files and do have the ability to capture personal data.

Session cookies, those that store page information, do not keep memory or code information about the user at the machine. That is, these are the “good cookies” of the Internet. Third-party cookies, also known as tracking cookies, on the other hand, do store data about site preferences and do pose more of a privacy risk because these cookies do track browsing habits and movements across the web. Although a third-party cookie might be less of a privacy risk, a web beacon poses more of a threat to web users. According to the Network Advertising Initiative (2012), “web beacons can be used for many purposes—including site traffic reporting, unique visitor counts, advertising auditing and reporting, and personalization.” As Julia Agwen (2010) examined, the reporting and personalization is more in-depth than we might think. What is troubling about the reporting is companies, including top websites, have the ability to identify the habits of an individual, including finding out, “what people are doing on a Web page, then instantly access location, income, shopping interests, and even medical conditions” (p. 2). Web beacons also have the ability to track how many clicks occur on the page and even when the mouse moves. Most of what we have come to know about trackers comes from third-parties—from advertisements and banners that are not part of the first-party page, meaning the ads come from another location other than the site. This means that with websites introducing banners and ads as a means to make money, other companies store third-party elements on machines. In a highly instructional video about third-party elements on the web, Clayton Miller (2008) described how companies use third-party cookies. In his video, he explained the process like this: Let’s say that you visit Yahoo! for information, and there is an advertisement for some
new product, and that ad installs a third-party cookie on your machine. Each time that you visit other websites that use that cookie file, the site searches for that cookie—once it identifies it is on your machine, it adds a new line of code to the file. The file can become inundated with code from all the sites you’ve visited that use that cookie. Companies that have access to that cookie can pull that information from the file and in turn use that data for a more customizable advertisement experience. Does this sound eerie and potentially exploitive? Well, in some cases, it is.

To be fair, not all third-party elements are created equal, and not all track online behavior. According to a Ghostery infographic titled “Know your elements (2014) there are five types of third-party trackers. “Advertiser: a tracker that delivers advertisements; Analytics: a tracker that provides research/analytics for website publishers; Beacon: a tracker that exists only to track user behavior; Widget: a tracker that provides some kind of page function (comment forms, “Like” buttons); and Privacy: a tracker that discloses data practices involved in delivering an ad.” Ghostery compiled data using their GhostRank platform (Protecting, 2012). This voluntary platform allows Ghostery to capture data about the trackers installed on machines to learn more about the major contenders in online behavioral advertising for those who use their plug-in. However, while trackers provide different functions, what is most concerning to all of us is the lack of information the companies who use these elements provide to users about what kind of personal data appears in the files installed on our machines. In the case of packaging and selling to other companies, what unique identifying information about invisible digital identities are circulating without our knowledge or control? Or, more importantly, what do our invisible digital identities show about who we are as creatures of habit and varied interests? Let’s put it another way: would you like for your grandma to know your invisible digital identity?

What is important is keep in mind about these tracking technologies is how developers in Silicon Valley are part of surveillance practices. The revelation of project Prism, a federal government project that allowed the NSA access to data in top-tier social sites like Facebook and Google, revealed how much of user privacy is lost because of web tracking technologies. Robert McMillan (2013), who wrote about the NSA scandal, reflected upon how Internet companies are part of the surveillance community,

Whatever Prism turns out to be, its public disclosure has brought attention to an uncomfortable fact of life for many of these internet companies: they are in the business of collecting and analyzing personal information, and that information is often of great interest to intelligence agencies. “I don’t actually believe that anyone at Google or Facebook or any ISP is being intentionally malicious,” says Moxie Marlinspike—a computer security expert who until January worked at Twitter—a company that was not named on the NSA Prism slides. “However, they are sort of in the surveillance business.” (para. 10)

Understanding how cookie development and tracking operates is crucial to knowing how a part of our online environments works, especially when we surf and write online. Given that Jay David Bolter (2001) argued that, “Writing technologies, in particular electronic writing today, do not determine how we think or how we define ourselves. Rather, they participate in our ongoing cultural redefinitions of self, knowledge, and experience” (p. 189), our writing technologies are redefining our experiences, in some ways, through digital surveillance and tracking technologies, especially about identity and virtual bodies. While we can limit third-party cookies on our machines through browser plug-ins and protection software, there is still some leakage of our personal data online. We may never be able to realize a web where tracking is not part of the package, but being educated about tracking technologies and how to limit the data stored and shared helps protect us, and ultimately our students, when we ask them to go online in the classroom.

2. Online privacy and surveillance tactics on the web

Moving into recommendations for teachers to use in educating students about surveillance tactics on the web, I offer how various corporations have tracked me on the Internet through multiple tracking technologies to demonstrate how much tracking occurs. To illustrate this, I used two ways to examine tracking software, the website [http://www.aboutads.info/choices/], and Ghostery—suggested to me by a colleague on Twitter. I use these two examples to explain the ways in which I have unknowingly had my online habits tracked and used for companies to better market how I view information on the web.

---

4 Digital rhetorician Tim Lockridge tweeted for me to explore Ghostery. I am indebted to him because this one tweet shaped the direction of this project and ultimately shifted my research agenda early in my doctoral studies.
The connection between cookies and web beacons link to notions of online privacy, which is a slight misnomer. We might think of online privacy in terms of our control over uploading, sharing, and deleting information when we choose to do so, but that is hardly the case any longer with tracking technologies. Sipior, Ward, and Mendoza (2011) pointed out that the notion of privacy “dates to the 1960s, when the issue of consumer privacy and data protection was new” (p. 12). Online privacy has come to mean our control over our information and the threat that is at the heart of privacy online is unseen. The placement, collection, and transmission of information from tracking technologies, without users’ knowledge, is what is most alarming with digital media use (Sipior, Ward, Mendoza, 2011, p. 14). Arguably, there are benefits as well as constraints to tracking technologies—i.e. more personalized advertising or rewards for interacting in virtual spaces—but users may want to opt-out of data tracking, especially if some tracking technologies reveal nuanced details about their online habits.

2.1. AboutAds.info and tracking technologies: Providing a list of trackers

AboutAds.info is the home of Digital Advertising Alliance’s (DAA) Self-Regulatory Program for Online Behavioral Advertising. According to the home page, the OBA applies “consumer-friendly standards to online behavioral advertising across the Internet” (Digital Advertising Alliance, 2010). The page also provides educational materials to consumers who want to learn more about cookies and various tracking technologies and serves as the hub for opting-out of behavioral advertising. One of the best educational resources listed on the site comes from a web page developed by David Whalen (2002), a senior Internet engineer, who has web industry experience and writes in numerous web-based applications. His site, [http://www.cookiecentral.com/faq/] provides a good overview of cookie fundamentals, including how to read a cookie file. Aboutads.info also provides a place to list complaints if users think that companies who are a part of the DAA have violated their privacy rights.

The site provides an opt-out of behavioral advertising. The opt-out page shows a program that runs through the browser to capture which companies have customized ads attached to the browser generated from tracking technologies. This means that through OBA, cookies are associated with browsers, not individuals. Each browser a person uses on a machine means returning to the opt-out page to learn what cookies are associated with that browser. For example, I run three browsers for various purposes—Internet Explorer, Firefox, and Chrome. I ran the opt-out script in each browser and found different results. I will give more detail in the next paragraph. Also associated with the page is a link to an informational web page named, “How Internet-based Ads Work.” From here, users can learn more about tracking technologies and the customized ads users see through their browser.

When a user opens the Opt-out page (2010), he or she is greeted immediately with a grayed-out box over top of the program that runs the browser for cookies. The message, “Testing Browser Support for Cookies. The functionality of this page requires that your browser allow both first and third party cookies” appears. The program runs for a brief period, and results of participating companies with customizable ads on the browser appears (Figure 1). From here, a user can look at the participating companies and customizable ads and then decide what to opt-out of from the site. When I ran the program in Firefox, I had 117 participating companies with 66 customizable ads. In Chrome, I had 117 participating companies with 30 customizable ads. In Internet Explorer, I had 116 participating companies with 94 customizable ads—all acting to create an invisible digital identity about me. In addition to providing the number of companies and customizable ads, the program also gave a drop-down abstract of each company with the company’s Website. For example, the abstract for Google, Inc. showed the following:

Google (www.google.com) operates the Google Display Network (comprising partner websites and some Google properties like YouTube), DoubleClick online ad serving products and the DoubleClick Ad Exchange, and Invite Media. These provide advertisers with the tools needed to plan, execute and analyze marketing programs with greater ease and efficiency, while enabling publishers to maximize their returns from online advertising. Note: Because Google uses DoubleClick and Invite technology, cookies placed by Google for behavioral advertising, including the opt out cookie, will appear as DoubleClick and Invite cookies. To learn more about how we collect and use information for online advertising, please visit http://www.google.com/intl/en/privacy.html

The opt-out page offers users and teachers means to learn more about the companies who have enabled ads on web browsers and to make more informed decisions based on the privacy practices of each company. For example, one company that appeared on my list caused concern—Lotame Solutions. According to Lotame’s (2012) privacy practice policy, their company collects a host of data from users including, “the date and time you visited a website, your browser
information, your IP address, your browsing behavior, your age and gender, your interests you express or imply at social networking sites or other websites you visit” (para. 9). On the surface, this language appears broad and not so intrusive. On a much deeper level, it’s not. Lotame Solutions is the same company that Julia Angwin wrote about in the Wall Street Journal in 2010. In the opening of the article, Angwin shared that a file code stored by Lotame Solutions on a 26-year-old female’s computer that showed details about her favorite movies, down to the titles of the movies, including her interests in entertainment news and quizzes. Lotame Solutions captured this data using web beacons. This left me thinking about the invisible digital identity Lotame Solutions created about me. More importantly, I wondered if the company would grant me access to the rich data portrait of my online activities. While this is an extreme example, and I would be remiss to note that not all companies collect this high level of detail, it is beneficial for Internet users to have a sense of the amount and detail companies collect, particularly if users are concerned about their online privacy.
2.2. Tracking the trackers: Ghostery

An alternative to tracking the trackers online is through the plug-in, Ghostery (Figure 2), which encourages users to learn, through a small box that appears at the upper-right side of the screen, about what companies are tracking their browsing habits each time they move from site to site. Unlike AboutAds.info, Ghostery provides users with real-time, up-to-the-minute information about trackers per page. Instead of users moving to the AboutAds.info page to see a list of trackers on the whole, Ghostery shows each tracker per page. Not only can users download Ghostery for five web browsers (Firefox, Safari, Google Chrome, Opera, and Internet Explorer), but there is also an option to download the plug-in for iOS for mobile web browsing. This makes Ghostery, overall, a good tracking-the-trackers plug-in to install because of its use across multiple browsers. While both AboutAds.info and Ghostery are similar, Ghostery provides information to users when each page they click on while surfing. In this way, Ghostery is an ever-present educational tool that users see while surfing the web.

Like AboutAds.info, Ghostery gives users the option to opt-out of online behavioral advertising. First, Ghostery allows users to see the invisible scripts that run in the background—web tags, bugs, and beacons—and allows users to see which trackers are collecting behavioral data. It then gives users the opportunity to learn more about the company with links to privacy practices through the Ghostery plug-in (Figure 3). The abstract information that Ghostery provides on the “Knowledge Page” is valuable to those of us who do not have the time or inclination to read through highly technical and, in some cases, hard-to-understand language about privacy practices. As Heidi McKee (2011) elsewhere questioned about reading privacy practices and the time it takes to read through each one, users would have to spend an inordinate amount of time reading through each privacy policy to understand how companies collect data. Admittedly, I do not have time to read each policy and rarely do. For this reason, Ghostery’s abstract of companies’ privacy polices gives the needed highlights of the data collected for users to make more informed decisions.

Both AboutAds.info and Ghostery use different methods for learning about which companies have installed cookies on machines for targeted advertising, yet Ghostery provides greater access to educational materials and visibility to the
Figure 3. Privacy abstracts provided by Ghostery.
invisible tracking technologies installed on the machine than AboutAds.info does. Ghostery does this through being present with each click of page. If there are third-party elements on websites, Ghostery immediately appears in a purple box to alert the user of the elements on the page. For example, when I went to my favorite music information website, Pitchfork, Ghostery immediately alerted me of six third-party elements the website uses. This real-time data helped me to understand what third party elements were installed on my machine versus returning to AboutAds.info every couple of weeks to learn if new elements had been added with new website visits.

3. How objects and humans create the invisible digital identity

Becoming educated about various types of first- and third-party elements used during browsing sessions is certainly the first step in learning about how companies construct an invisible digital identity. Even with the knowledge of good and bad cookies and elements, I am still concerned about what is unknown to me—the information that companies gather from my machine that they use for their purposes—and whether it’s internal or external by selling my browsing habits to other companies. The surveillance tactics by companies driven by profit harks back to Michel Foucault’s (1977) notion of the panoptic eye and how it became the apparatus of social control, discipline, and a way to categorize and observe at singular levels. Foucault’s theory of discipline and social control is useful for theorizing ways 19th and even 20th-century institutional bodies isolate and punish individuals as a cultural practice. It is also important to keep in mind that Manual Castells (2000) elsewhere noted that power has shifted from institutions to the network. Thus, a 21st-century networked panoptic theory is needed to describe how power flows within the networked relations not only through people, but also through objects. In many ways, Foucault’s theory of control provides a foundation for control, yet the theory is too human-centric with regards to the recent advancement of digital networks. Or, to put it another way, his theory does a great job for accounting for the institutional control of bodies, and a turn to the complexities of networks and how control functions in varying systems is needed. I argue that digital rhetoricians and digital writing teachers need a theory that places both objects and humans in the same ontological state that helps shift toward seeing objects as equal in force and weight as humans. Because networked culture is as much about the hardware, software, and immaterial algorithms as it is about the people and the cultural codes embedded within those systems, a theory that moves past a binary between humans and objects as tools helps usher in new lines of research and conversations about object agency.

3.1. Code culture and object-oriented rhetoric

In code culture, humans write the code, and the code works through processes and performs operations. Code operates as both a form of expression and as a process; it’s recursive nature allows machines to both read and write code simultaneously, thus making code not only a type of apparatus with which to work, but also a language that is reflexive. As Ben Williamson (2013) noted, “Code acts. It does work in the world” (para. 5). It’s not just a computer programmer using the tool of code to make decisions; code functions to process on its own without direct human interaction. For example, Rob Kitchin and Martin Dodge (2011) argued that code is in a sense alive, “because it means code can make things do work in the world in an autonomous fashion—that is, it can receive capta and processes information, evaluate situations, make decisions, and, most significant, act without human oversight or authorization” (p. 5). This makes code its own object, thereby having its own ontological state. Recalling Foucault’s panoptic prison apparatus, it’s helpful to keep in mind that contraption remained a tool for humans to observe and later make judgments about, but did not necessarily account for the role of objects other than within a subordinate role to human examination. Code, a non-material object, has much to bear upon shaping the identity of people in certain digital spaces because of its recursive nature as both a readable, writable, and most importantly, executable machine language, capable of existing and shaping ways people engage in online spaces. Additionally, code, while invisible to non-programmers or inaccessible to those who do not read code, still performs simple and complex actions in software programs that intersect with complexly layered cultural ecologies of human life. As Adrian Mackenzie (2003) wrote,

Code runs deep in the increasingly informatically regulated infrastructures and built environments we move through and inhabit. Code participates heavily in contemporary economic, cultural, political, military, and governmental domain. It modulates relations within collective life. It organizes and disrupts relations of power. It alters the conditions of perception, commodification and representation. (p. 3)
Not only does code perform actions, but also has the ability to change the ways in which people interact with code. Thus, it’s here we might begin to say that code not only has suasive properties, but also is rhetorical in nature.

Alex Reid (2012) already began to explore how objects have rhetorical properties through object-oriented rhetoric—a meshing from Graham Harman’s object-oriented philosophy, i.e. placing objects at the center of being alongside humans. Reid (2012) noted that rhetoricians do not quite yet know how to work with object-oriented rhetoric yet and stated, “But the place we’d probably begin is with recognizing conventionally we understand rhetoric to be the study of human symbolic action. Object-oriented rhetoric (OOR) would ask what would it mean to understand rhetoric as non-human, and something might not require symbolic action.” He went on to note that if digital rhetoricians applied object-oriented philosophy to rhetoric, “we [could] think about the kinds of challenges, and gaps of misunderstanding and incomplete relations, and how we might try to mitigate those through rhetorical acts” (Reid). An OOR approach provides digital rhetoricians with an escape from the binary between humans and machines, and gives way to a network of all elements cast as objects or a flat ontology. Manuel DeLanda (2002) defined this concept as, “...an approach in terms of interacting parts and emergent wholes leads to a flat ontology, one made exclusively of unique, singular individuals, differing in spatio-temporal scale but not ontological status” (p. 41).

In underpinning a theoretical transfer of object-oriented ontology/philosophy into rhetoric, there is a sense of having to incorporate the study of action and/or persuasion into an object-oriented rhetorical position. This is especially so since an object-oriented ontology only allows for the philosophizing of the nature of being and even the nature of difference among being. Harman’s object-oriented philosophy, as it has been understood, turns from Kant’s Copernican Revolution, and views objects as existing independent of human awareness. While the philosophy does take into consideration relations among objects and relations between humans and objects5, I argue that the relations under discussion in OOO circles are not the type of relations that allow for suasive forces to emerge under a rhetorical application. Therefore, I see that using some of Bruno Latour’s (2005) philosophies helps position an object-oriented rhetoric.

An incorporation of Latour’s actor-network theory (ANT) to account for the relations between those objects and even humans with object-oriented ontology helps us move closer to the suasive nature of computer algorithms, as well as come to better understand the tracking technologies used in certain online spaces. As Ian Bogost (2012) argued of ANT, “Latour allows for the uncontrollable existence of things at all scales. But in the networks of actor-network theory, things remain in motion far more than they do at rest, as a result, entities are de-emphasized in favor of their couplings and decouplings” (p. 7). While Bogost critiqued ANT to position his use of object-oriented ontology (OOO) to allow ANT to recede to the background in favor of OOO in the foreground, digital rhetoricians might find an ANT coupling with OOO fruitful for theorizing how persuasion is a type of action and relation between and among objects and humans in networks. Such a coupling may be especially worth scholarly attention given that computer algorithms and tracking technologies create invisible digital identities. As such, persuasion as action-oriented, and arguably as an object and human phenomenological position, helps humans see the guiding centrism and perceptions at play. The relations between the objects become the emphasis, then, within a network. Additionally, such a theory allows digital rhetoricians to conceive of how objects can enter into a suasive appeals through the assemblage of code, objects, actors, and materials that stabilize and destabilize according to the in- and out-put flows of the network(s). The immaterial properties that flow through the material network, i.e. the algorithms and codes constantly fluctuate and e- and de-volve through the relations of the presence and absence of other objects.

Using OOO and ANT to move into an object-oriented rhetorical theory helps better describe the networks of digital surveillance in online spaces as well as the computer algorithms and tracking technologies that collect data about users. An object-oriented rhetoric also helps destabilize the human-centric position of Foucault’s panopticon and positions objects and humans along assembled and distributed networks to see the nudges and full on pushes in networks when multiple objects and people collide. OOR helps position us to acknowledge ways computer algorithms, the very ones that track us online, persuade us to click on advertisements or respond to certain elements in social media spaces beyond just seeing algorithms as subordinate to a human position, but as equal in existence, and therefore warranting further exploration into computer code. Studying cookies and web beacons provides digital writing researchers and teachers with knowledge that virtual objects are just as important and can have significant freight in interaction with

---

5 As having a notion of equally existing (Bryant, 2012, para. 8), but not necessarily being equal in existence as some objects have more to bear in their relations.
humans in virtual spaces. The objects not only have an existence, but also provide data and persuade other codes and people to act. With that said, we also cannot ignore the messy realities of how ideological positions are embedded in tracking technologies. This notion echoes Judy Wajcman’s (2004) theory of technofeminism and the very real sexual politics involved in the material production of objects and how that can affect women and all people in physical as well as virtual spaces. Moreover, digital users and writers of the Internet cannot simply ignore the globalized political economy that so heavily relies upon computer code and architecture, and thereby shapes online discourse and design patterns. As digital rhetoricians and as digital writing teachers, we can become better informed about invisible digital identities, how material and immaterial objects operate behind the networked veil, and in turn, inform our students who write in online spaces.

One final thought digital rhetoricians and teachers might consider worthwhile: as we turn our attention to teaching our students about tracking technologies and sites like AboutAds.info and Ghostery, we are participating in what Steve Mann, Jason Nolan, and Barry Wellman (2003) dubbed, sousveillance, from the French words “sous” (below) and “veiller” to watch (p. 332). This converse panopticism, us watching the watchers, gives us some sense of control over online behavioral advertising. Our invisible digital identities—stored, collected, and transmitted—start to become visible, and through the tracking websites mentioned in this article, we can perhaps see more of the data iceberg that companies have collected about us. Our relationship to surveillance on the web becomes inverted with a redistribution of power and control. With companies looking at us, we can also look at them and decide whether the companies who use third-party elements do so in a way that lines up with our notions of privacy and data sharing on the web. In effect, we develop agency as well as a new understanding of digital literacy—crucial steps that can lead to empowerment and protection in online spaces.

4. Educating our students: Our responsibilities for classroom web use

Each time we enter online spaces, our movements are recorded and, in some cases, tracked. Thus, the question becomes how might we best inform our students about the types of tracking technologies and invisible digital identities constructed by companies from web use? To be certain, web-tracking technologies are not going to disappear, and with rapid developments in technology and marketing tactics, we can be sure that we will be tracked more as the years pass by, and to some degree, there are benefits to providing some user data to companies to better tailor our web experiences. Thus, we have to educate ourselves to understand the technology developments, to learn what files companies install on our machines, and then to separate the good from the bad. Beyond that, I recommend three additional steps: 1) educating our students about these technology developments; 2) sharing with students sites that track the trackers, and 3) having students learn about privacy policies to make informed decisions about data collection practices of websites.

As teachers integrate conversations about technology developments with third-party elements in their classrooms, we are also educating and providing safe spaces for our students. Our guiding instructions with asking students to get online, even to a site like Dictionary.com to access definitions, provides us with the opportunity to discuss the invisible digital identity on the web. The contradictions between the good and the bad third-party elements, with showing students how some websites track their movements, even asking students to log in to the Blue-Kai Registry to see their collected demographics, habits, and interests, helps students interrogate their invisible digital identity. Having students examine how companies use OBA can help students understand the underbelly of the Internet—a place where personal data collection is used to shape their experiences online through various interfaces and that through personalization of advertisements, inequities of class, race, gender exist (see Selfe & Selfe, 1994).

Once we ask students to engage in sites like AboutAds.info or Ghostery, we are asking students to become more informed, critical observers and assessors of information on the web. Once students install the plug-in of Ghostery, for example, on one browser, leading them through different websites like dictionary.com, Yahoo!, MSN, and eBay are useful activities for students to see the different companies that have installed files on their computers. Paired with this activity, teachers can also ask students to open Ghostery and learn about all the sites with OBA files on their machines, and then task students to read the brief privacy policy abstracts associated with each company. This can even extend to a larger project where students interrogate OBA files and explore the networked relations companies who use other files to capture data and build profiles of users on the web.

When teachers begin the task of educating students about OBA and tracking technologies, a heuristic might be helpful. Thus, I offer some extensions that speak to the teaching of invisible digital identity and OBA technologies.
1. How do I develop awareness for my students about online behavioral advertising?
2. How will my teaching of tracking technologies and online behavioral advertising support university, departmental, and my learning outcomes of the course?
3. What tools will I use to show students about tracking technologies?
4. How am I providing safe spaces for students when they go online to various websites that use tracking technologies?
5. How can I help students begin to harness some degree of control over OBA by becoming informed and possibly opting-out of some OBA trackers?
6. What impact will occur when students learn about their invisible digital identities? Will students feel comfortable sharing the details of their “hidden” life with others? How might I provide alternatives for people who may not feel comfortable sharing what has been branded about them?
7. Will my department support my discussions about invisible digital identity in my classroom?
8. Once students learn about their invisible digital identities, what activities and/or projects can I develop so their information gathering is meaningful?
9. How will opting-out of some OBA trackers affect my students’ abilities to access information and surf the web?
10. How will this lead to student empowerment to share their knowledge with their peers outside of the class?

While this brief heuristic touches on broad concerns of university expectations, department expectations, and pedagogical beliefs, it also focuses on more narrow areas of exploration. Nevertheless, it represents a starting point that teachers can use to branch out and develop further questions that are appropriate for their institution, department, and students.

5. Taking back our digital identities

Ever since cookie development in the 1990s, people who use the web have been concerned with online privacy, i.e. how to protect their personal information and data while enjoying the benefits of a connected digital life. As computer technology has developed from closed systems to open systems of staged development where advertisers have sought ways to market products strategically, there has been concern about how companies access personal data through tracking technologies like flash cookies and web beacons—and most importantly, what those companies do with that information. Granted, visiting a site like BlueKai—whose sole purpose is to collect big data—is problematic because their interests are more aligned with profit than with protecting consumers; however, the company does make efforts to inform consumers about the information stored on their machines through the BlueKai Registry. Certainly, we are never going to realize a web free of tracking technologies, but as educators, we do have a responsibility of teaching our students about the types of data companies collect when we ask them to go online in our classrooms.

While there have been, for some time, spaces online that are open-source and do not use tracking technologies—such as the newer search engine, DuckDuckGo—with these spaces being perhaps ideal for educational purposes, digital writing teachers have to teach not only ourselves but also our students about the types of tracking technologies and surveillance habits of organizations online. This guided conversation can happen alongside talks about visible digital identity. When we ask students to create social media profiles for course projects, engage in template-driven website creation, or even just surf the web for educational purposes, it is critical that we also talk about how data about online habits and behaviors are stored, collected, and used. For example, while teachers may advocate to create anonymized social media accounts to protect students’ visible digital identities (their legal names, identities, etc.) for concerns over stalking, how do such accounts collect or expose an invisible digital identity?\(^6\) In short, teachers need to keep both identities in mind when asking students to use social media or even Google products.

The implications concern how everyone can continue to interact in online spaces in safe ways and understand how our invisible digital identities are constructed through surfing habits. Those implications include responsibilities to

---

\(^6\) To protect both visible and invisible digital identities while online and through mobile app technologies, it is advisable to use virtual private networks (that do not log IP addresses) since may popular sites log IP addresses, block third-party tracking cookies through browsers, and install tracking technology software. For more advice, including creating PGP keys and using encryption software, visit Electronic Frontier Foundation online.
act and teach students about how to protect their identities online. It is up to all of us, as teachers and researchers, to talk about invisible digital identities with each other and our students. Thus, future lines of research in this area might further expose the detailed data companies collect from users, or it may turn to learning more about which companies are the most egregious with collecting detailed data and in turn sell our personal data for a profit, all in the name of better advertising. Additionally, theoretical and empirical research into invisible digital identities and the effects they have upon our students is needed. We may begin to chart what digital surveillance and the invisible digital identity means for critical digital literacy, with updating educational policy position statements on digital literacy. With our colleagues who work in cognitive studies and writing processes, future research may study the effects of the invisible digital identity and web customization on a writer’s cognition, writing processes, and habits. And, finally, within our departments, we might embed the invisible digital identity into our curriculum, getting people to think about what they do, why they do it, and how they can navigate the Internet to allow for interrogation of the ideological and material weight of these spaces. No matter what future research holds, we do have time now to start talking with our students about their invisible digital identities and how the assemblages of digital networks forecast object and human relations as central to interacting virtually.

References


