

THE PANOPTIC GAZE OF WEB SEARCH ENGINES: GOOGLE AS AN  
INFRASTRUCTURE OF DATAVEILLANCE

Michael Zimmer  
Department of Culture & Communication  
New York University

Introduction

In January 2006 it was revealed that the U.S. Justice Department asked a federal judge to compel the web search engine Google to turn over records on millions of its users' search queries as part of the government's effort to uphold an online pornography law (Hafner & Richtel, 2006; Mintz, 2006). Google resisted, but America Online, Microsoft and Yahoo! complied with similar government subpoenas of their search records (Hafner & Richtel, 2006). More recently, America Online released over 20 million search queries from 658,000 of its users to the public in an attempt to promote research on search engine usage (Hansell, 2006). Despite AOL's attempts to anonymize the data, individual users were identifiable based solely on their search history, prompting one to remark "My goodness, it's my whole personal life...I had no idea somebody was looking over my shoulder" (Barbaro & Zeller Jr, 2006). Together, these events brought to light the fact that search engine providers keep detailed records of users' searches, and created anxiety among searchers about the presence of such systematic monitoring of their online information-seeking activities (Barbaro & Zeller Jr, 2006; Hafner, 2006; Levy, 2006; Maney, 2006).

The freedom to move through both physical and intellectual space is a central theme of various American mythologies, such as the desire to explore unknown frontiers and acquire new knowledge, the overcoming of artificial barriers of distance for mass communication and commerce, and the ability to control one's relations and position in the world. Such myths become embodied in the set of values deemed vital for the success of our society, including privacy, autonomy and liberty. The emergence of systematic modes of data surveillance – otherwise referred to as “dataveillance” (Clarke, 1988) – within our spheres of mobility threaten the preservation of these fundamental values. Dataveillance in spheres of mobility can take many forms, including the use of radio frequency identification (RFID) tags in consumer products, the monitoring of vehicles as they travel along the highways, or the use of facial recognition cameras in public spaces. This chapter will examine the particular dataveillance threats of web search engines, paying specific attention to the dominant search engine Google, and will reveal how the aggregation of one's online information-seeking activities contributes to the creation of a panoptic gaze of everyday surveillance, inflaming a growing environment of discipline and social control.

This chapter is divided into four parts. Part one describes the role of web search engines as the prevailing information interface for accessing the vast amount of information available on Internet, concluding that search engines are the “center of gravity” for navigation within this vital sphere of information. Building from Foucault's notion of the “panoptic gaze,” the second part of the chapter introduces the concept of dataveillance, paying particular attention to the functioning of power through data accumulation and the role of information technology. Part three provides a brief technical analysis of Google's diverse suite of products, revealing how the integration of persistent web cookies, detailed server logs, and personal user accounts within and

across these products provides Google a powerful infrastructure of dataveillance to monitor, record and aggregate information about their users' online activities. Finally, part four concludes with a discussion of how Google's particular infrastructure of dataveillance poses a threat to the unencumbered navigation the Internet, harboring concerns over its role in the exercise of disciplinary power, panoptic sorting of its users, and the challenges of resisting its "gravitational pull" in the face of default settings which require the sharing of information.

### Web Search as the Center of Gravity

As the Internet has become increasingly important to modern citizens in their everyday lives (see Horrigan & Rainie, 2006), *web search engines* have emerged as today's prevailing information interface for accessing the vast amount of information available on this global network. According to the Pew Internet & American Life Project, 84% of American adult Internet users have used a search engine to seek information online (Fallows, 2005, p. 1). On any given day, more than 60 million American adults send over 200 million information requests to web search engines, making searching the web second the second most popular online activity (behind using e-mail) (Rainie, 2005). Originally designed to provide easy access to Internet websites, search engines now provide gateways to online images, news reports, Usenet archives, financial information, video files, e-mail and even one's desktop files. Recently, search engine providers, such as Google, have started to digitize items in the "material" world, adding the contents of popular books, university libraries, maps, and satellite images to their growing, searchable indices. Reflecting on the rapid emergence of search-related applications, Silicon Valley venture capitalist Roger McNamee noted that "search is the new center of gravity for the computer industry" (McNamee, 2005). The same can be said more generally for the role of

search engines as today's dominant information interface: *Search engines have become the center of gravity for people's everyday information-seeking activities.*

Consider, for example, the web search engine Google. Google has become the prevailing interface for searching and accessing virtually all information on the Web. Originating in 1996 as a Ph.D. research project by Larry Page and Sergey Brin at Stanford University (see Brin & Page, 1998; Page et al., 1998), Google's web search engine now dominates the market, processing over 2.8 billion search queries in July 2006, nearly half of all web searches performed (Nielsen//NetRatings, 2006).<sup>1</sup> Google's mission, stated quite simply and innocuously, is to "organize the world's information and make it universally accessible and useful" (Google, 2005a). In pursuit of this goal, Google has developed dozens of search-related tools and services to help users organize and use information in multiple contexts, ranging from general information inquiries to academic research, news and political information, communication and social networking, personal data management, financial data management, shopping and product research, computer file management, and enhanced Internet browsing. Consequently, users increasingly search, find and relate to information through Google's growing information infrastructure of search-related services and tools.<sup>2</sup>

---

<sup>1</sup> Nielsen/NetRatings figures represent U.S. searches only, and include local searches, image searches, news searches, shopping searches and other types of search activity from Google's various services. If only web searches at [www.google.com](http://www.google.com) are considered, Google's share increases to 60% (Sullivan, 2006).

<sup>2</sup> Yahoo!, and to a lesser extent, Microsoft and AOL, also offers search-related tools beyond just locating relevant websites. Google, however, remains the clear market leader at 49.2% of all search activity, with Yahoo! following at 23.8% and MSN at 9.6%. Given their strong dominance of the overall marketplace, and recognition as the "gold standard" in search engine practices and innovation (Clark, 2006; Hellweg, 2002) Google will be the primary focus on this study.

The emerging social and cultural impacts of this increasing reliance on search engines are being studied from a variety of disciplines. Scholars have explored the biases of search engine results (Introna & Nissenbaum, 2000; Diaz, 2005), the political economy of the search engine marketplace (Van Couvering, 2004), the legal ramifications of search engine practices (Elkin-Koren, 2001, #4881; Goldman, 2005), the structure of user queries and their searching skills (Hargittai, 2002; Jansen et al., 2000), the practice of paid placement of search results (Jansen & Resnick, 2005; Wouters, 2004; Zimmer, 2006), and general user awareness and trust in how search engines work (Fallows, 2005; Marable, 2003). Scholarly attention also been paid to the *ethical* issues related to search engines (Nagenborg, 2005), including discussions of the privacy issues related to search engine practices (Hinman, 2005; Tavani, 2005). However, most treatments of the privacy implications of web search engines have tended to focus on how search engines provide improved access to personal information that happens to exist online – the erosion of “security through obscurity” in the face of ever-expanding search engine indexes (Ramasastry, 2005; Swidey, 2003). While such concerns demand attention, it is crucial to look beyond the privacy implications of what kind of personal information about other people that can be *found* via search engines and examine what kinds of personal information is *collected* when users rely on search engines for their information-seeking activities.

The majority of web searchers are not aware that search engines have the ability to actively track users’ search behavior (Fallows, 2005, p. 21; Kopytoff, 2006). For many, this ability first became apparent when news broke of the Department of Justice’s legal battle with Google in early 2006, followed by the release of thousands of search records by AOL later that year. In response to the growing anxiety over the surveillance of search engine use, various tools and strategies emerged to help hide or obfuscate one’s web search activity from being easily

tracked and monitored (Howe & Nissenbaum, 2006; Schoen, 2006; Singel, 2006). Such efforts, while important, tended to either require a certain level of technological sophistication (i.e., the use of anonymous routing services such as Tor (Zetter, 2005)), suggest the blocking of search engine cookies which could prevent other desirable services from working properly, or focus only on keeping one's *web searches* from being tracked, ignoring the myriad of other opportunities available for web search engine providers to collect detailed information about its users. As search engine providers, like Google, continue to create complex information infrastructures that connect various products and services through the use of persistent web cookies or universal logins, they increase their ability to collect and aggregate a much wider array of personal information about their users than just their web search queries. As search engines become the center of gravity of user's information-seeking needs, their gravitational pull, to continue the metaphor, captures an increasing amount of personal information about those users, resulting in a robust *infrastructure of dataveillance* focusing a pantopic gaze on users as they engage in their everyday information-seeking activities online.

### The Panoptic Gaze of Dataveillance

According to sociologist David Lyon, surveillance is the “collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered” (Lyon, 2001, p. 2). Surveillance “tries to make visible the identities or the behaviors of people of interest to the agency in question” (Lyon, 2002, p. 2). Surveillance, then, encompasses a diverse range of activities and processes concerned with scrutinizing people, their actions, and the spaces they inhabit. Surveillance, of course, has existed for centuries, and its methods have been continuously refined to broaden its reach and

effectiveness. One notable refinement is English philosopher Jeremy Bentham's model penitentiary, the Panopticon (Bentham, 1995). Conceived in 1791, Bentham's Panopticon prison was designed to maintain (by allusion, if not by fact) perpetual surveillance of its inhabitants: by placing prison guards in central tower with a one-way observation system surrounded by rooms for those to be watched, the subjects were unable to determine when they were being watched. Through this unique architectural design, Bentham believed that the constant threat that one could be surveilled at any time would force the subjects to internalize the effects of surveillance:

The more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose of the establishment have been attained. ... This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he [the watched] should *conceive* himself to be so. (Bentham, 1995, p. 3)

Through such an arrangement, Bentham believed disciplinary power would be automatic, and thus exercised with minimal effort, or, as Michel Foucault later reflected, the Panopticon would “induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power” (Foucault, 1977, p. 197). This automatic functioning of disciplinary power, then, manifested itself through a *panoptic gaze*:

There is no need for arms, physical violence, material constraints. Just a gaze. An inspecting gaze, a gaze which each individual under its weight will end by internalizing to the point that he is his own overseer, each individual thus exercising this surveillance over, and against, himself. A superb formula: power exercised continuously and for what turns out to be a minimal cost. (Foucault, 1980, p. 155)

For Foucault, the Panopticon became a “generalizable model of functioning; a way of defining power relations in terms of the everyday life of men... it is in fact a figure of political technology that may and must be detached from any specific use” (Foucault, 1977, p. 205). He viewed the Panopticon as the quintessential disciplinary apparatus of modern society, where the panoptic gaze extended beyond Bentham's specific architectural form, and manifested itself in various contexts of everyday life: the home, the school, the hospital, the workplace, and so on.

The gaze of the Panopticon expands to become “a whole complex mechanism, embracing ... stricter methods of surveillance [and] more efficient techniques of locating and obtaining information” (Foucault, 1977, p. 77). By suggesting a link between the Panopticon and “more efficient techniques of locating and obtaining information,” Foucault reveals a pivotal feature of the modern panoptic gaze: the functioning of power through data accumulation.

For Foucault, the functioning of the Panopticon depended on perpetual surveillance and the “continuous registration, perpetual assessment and classification” of those under its gaze (Foucault, 1977, p. 220). Oscar Gandy recognized this perpetual and disciplinary gaze of personal data accumulation when he warned of the “panoptic sort” (Gandy, 1993), whereby individuals are continually identified, assessed and classified for the purpose of coordinating and controlling their access to consumer goods and services, a process he insists is inherently discriminatory. Gandy’s concern with panoptic sorting has been expanded beyond the consumer realm into a broader social milieu (Lyon, 2003a), where the notion of “social sorting” highlights the growing drive in our modern surveillance society for identification and classification. Since classification has been shown to be closely entwined with the exercise of power (Bowker & Star, 1999; Foucault, 1971; Suchman, 1997), the consequences of panoptic and social sorting – and the panoptic gaze which form their foundation – present issues of “deep discrimination...and social justice” (Lyon, 2003b, p. 1).

The catalyst triggering both Gandy and Lyon’s anxiety was the rapid emergence of a complex set of technologies and practices that involve “the collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers (Gandy, 1993, p. 15). This panoptic apparatus resembles what is now referred to as *dataveillance*, defined as both “the massive collection and storage of vast

quantities of personal data” (Bennett, 1996, p. 237) and “the systemic use of [such] personal data...in the investigation or monitoring of one or more persons” (Clarke, 1988, p. 499). Clarke’s (1988) introduction of the term dataveillance revealed how the disciplinary gaze of the panopticon has extended from a single, centralized source (Bentham’s guard tower) into the realm of advanced information technologies and computer databases that facilitate the collection and exchange of information about individuals. Yet, the resulting effect of dataveillance’s technologically distributed panoptic gaze matches that of Bentham’s Panopticon envisioned two hundred years before – the internalization of power:

An administrative apparatus that has data available to it from a wide variety of sources tends to make decisions on the person's behalf. Hence, a further, more abstract, yet scarcely less real impact of dataveillance is reduction in the meaningfulness of individual actions, and hence in self-reliance and self-responsibility. Although this may be efficient and even fair, it involves a change in mankind's image of itself, and risks sullen acceptance by the masses and stultification of the independent spirit needed to meet the challenges of the future. ...In general, mass dataveillance tends to subvert individualism and the meaningfulness of human decisions and actions. (Clarke, 1988, p. 508)

Since Clarke’s first conceptualization of dataveillance almost twenty years ago, advances in digital networking, data storage capacity and processing power have enabled previously unimaginable levels of interconnectivity, aggregation, and real-time analysis of a wide array of personal information. Increasingly, everyday interactions with health care providers, online retailers, highway tollbooths, local grocery stores and libraries result in the collection, analysis, storage and sharing of information about one’s address, purchasing habits, age, education, health status, travel activity, employment history, phone numbers and much more, into what legal scholar Daniel Solove (2004) calls “digital dossiers.” The rising ubiquity of dataveillance in everyday life and resultant sophistication of “digital dossiers” has led to widespread concern over the social and value implications of this new digital panoptic gaze (see, for example Elmer, 2004; Gandy, 1993; Garfinkel, 2000; Lyon, 2003a; Lyon & Zureik, 1996; Regan, 1995; Solove,

2004; Staples, 2000;). As Clive Norris and Gary Armstrong argue in their study of the introduction of computer databases into video surveillance systems, the pervasiveness of digital dossiers (or, using their term, “digital personas”) have “more than just an electronic existence: they have concrete material effects” (Norris & Armstrong, 1999, p. 221). Such effects relate not only to personal privacy, but also issues of discrimination, social justice, and personal freedom.

Law professor Michael Fromkin (2000) summarizes these effects best:

Reams of data organized into either centralized or distributed databases can have substantial consequences beyond the simple loss of privacy caused by the initial data collection, especially when subject to advanced correlative techniques such as data mining. Among the possible harmful effects are various forms of discrimination, ranging from price discrimination to more invidious sorts of discrimination. Data accumulation enables the construction of personal data profiles. When the data are available to others, they can construct personal profiles for targeted marketing, and even, in rare cases, blackmail. For some, just knowing that their activities are being recorded may have a chilling effect on conduct, speech, and reading.

...A further danger is that the government or others will attempt to use the ability to construct persona profiles in order to predict dangerous or antisocial activities before they happen. People whose profiles meet the criteria will be flagged as dangerous and perhaps subjected to increased surveillance, searches, or discrimination. (pp. 1469-1471)

The role of modern information and communication technologies within infrastructures of dataveillance cannot be understated: frequent shopping cards connect purchasing patterns to customer databases (Ward, 1998), intelligent transportation systems enable the tracking and recording of vehicles as they travel the highways (Bennett et al., 2003; Zimmer, 2005), electronic key cards manage access to locations while creating a record of one’s movements (Stalder & Lyon, 2003), and biometric technologies digitize one’s intrinsic physical or behavioral traits for automated identification and authentication (Agre, 2003; Brey, 2004). Recently, the Internet has emerged as not only a revolutionary technology for communication, commerce and the distribution of information, but also as an ideal infrastructure of dataveillance, enabling the widespread monitoring and collection of personal and identifiable information about its millions

of users (Electronic Privacy Information Center, 1999). The privacy and surveillance concerns with various Internet technologies have been well documented and debated, ranging from the use of web cookies and tracking bugs (Bennett, 2001; Kang, 1998; Mayer-Schönberger, 1997), the emergence of spyware and digital rights management systems (Cohen, 1996, 2003), workplace monitoring of electronic communications (Froomkin, 2000), the aggregation and data-mining of personal information available online (Garfinkel, 2000; Solove, 2004), and the widespread monitoring of Internet traffic by law enforcement agencies (Regan, 2001; Ventura et al., 2005). The design and deployment of each of these new Internet technologies represents an expansion of the panoptic gaze of dataveillance online, which is intensified with the growing power and ubiquity of web search engines and the larger information infrastructures on which they rely. The following section will reveal how the integration of persistent web cookies, detailed server logs, and personal user accounts within and across Google's diverse suite of products provides it a powerful infrastructure of dataveillance to monitor, record and aggregate information about their users' online activities.

### Google as an Infrastructure of Dataveillance

Since the first search engines started to provide a way of interfacing with the content on the Web, there has been a drive for the "perfect search engine," one that has indexed all available information and provides fast and relevant results (see Andrews, 1999; Gussow, 1999; Kushmerick, 1998). A perfect search engine would deliver intuitive results based on users' past searches and general browsing history (Pitkow et al., 2002; Teevan et al., 2005), knowing, for example, whether a search for the keywords "Washington" and "apple" is meant to help a user locate Apple Computer stores in Washington, D.C. or nutritional information about the

Washington variety of the fruit. Given the current environment of advertising-support search engines, a perfect search engine would also be able to deliver only advertisements that are deemed useful or desirable for that particular user (Hansell, 2005). Web journalist John Battelle summarizes how a perfect search engine might provide a nearly perfect answer to every query:

Imagine the ability to ask any question and get not just an accurate answer, but your perfect answer – an answer that suits the context and intent of your question, an answer that is informed by who you are and why you might be asking. The engine providing this answer is capable of incorporating all the world’s knowledge to the task at hand – be it captured in text, video, or audio. It’s capable of discerning between straightforward requests – who was the third president of the United States? – and more nuanced ones – under what circumstances did the third president of the United States forswear his views on slavery?

This perfect search also has perfect recall – it knows what you’ve seen, and can discern between a journey of discovery – where you want to find something new – and recovery – where you want to find something you’ve seen before. (Battelle, 2004)

Search engine engineers recognized early on the importance of designing the perfect search engine, such as Google co-founder Sergey Brin’s assertion in the company’s very first press release that “a perfect search engine will process and understand all the information in the world...That is where Google is headed” (Google, 1999). When later asked what a perfect search engine would be like, Brin replied quite simply, “like the mind of God” (quoted in Ferguson, 2005, p. 40).

To attain such an omnipotent and omniscient ideal, a search engine must also be able to, borrowing Battelle’s wording, provide results that suit the “context and intent” of the search query, and must have “perfect recall” in order to deliver personalized and relevant results that are informed by who the searcher is. Attaining such recall requires search engine providers to collect as much information about their users as possible – they must engage in dataveillance of their users’ online activities. To accomplish this, Google, like most web search engines, maintains detailed server logs recording each web search request processed through their search engine and

the results clicked (Google, 2005b, 2005c). While Google's server logs include the IP address of individual queries, Google also relies heavily on web cookies to help differentiate users and track activity from session to session.<sup>3</sup> The most widespread use of cookies by Google is for tracking the usage of Google's products in order to "improve the quality of our service" (Google, 2005c). By including web cookie information in their server logs, Google, like many web providers, is able to better distinguish between users of the website, overcoming some of the limitations of relying solely in IP addresses.

However, as the privacy concerns of the use of cookies to track users' online activities increases (Kristol, 2001; Mayer-Schönberger, 1997; Schwartz, 2001), their usefulness to web providers diminishes. Users increasingly take advantage of software and browser features that make it easier to view, delete and block web cookies received from the sites they visit (McGann, 2005; Mindlin, 2006). To compensate for the growing unreliability of cookies to maintain accurate records of user activities, web providers increasingly urge users to register with the website and login when using the services (Ho, 2005, pp. 660-661; Tec-Ed, 1999).<sup>4</sup> Google started experimenting with products and services that required users to register and login in early 2004, including personalized search results, e-mail alerts when sites about a particular topic of interest are added to Google's index (Kopytoff, 2004). Many other services requiring a Google Account soon followed, and while all that was required to create a Google Account is a valid e-

---

<sup>3</sup> A web cookie is a piece of text generated by a web server and stored in the user's computer, where it waits to be sent back to the server the next time the browser accesses one of its webpages.

<sup>4</sup> When a user supplies a unique login identity to a web server, that information, along with the current cookie ID, is stored in each log file record for that user's subsequent activity at the site. By tying certain functionality of the site to being logged in, the user is compelled to accept the web cookie for that session. Even if the user deletes the cookie at the end of the session, by logging in again at the next visit, a consistent record for the user in the server log can be maintained.

mail address, the submission of additional personal information is often necessary to take full advantage of Google's suite of products. Google's encouragement of the creation of Google Accounts, combined with its use of persistent web cookies, provides the necessary architecture for the creation of detailed server logs of users' search activities.

While public attention has recently focused on the ability of Google to track user's search history in detailed server logs (Hafner & Richtel, 2006; Mintz, 2006), less attention has been paid to how Google can also monitor and aggregate activity across the myriad products and services that make up their larger web search information infrastructures. Google's searchable index has expanded to include not only websites, but also images, news reports, Usenet archives, and video files. Additionally, Google has begun digitizing the "material world," adding the contents of popular books, university libraries, maps and satellite images to their growing index. Users can also search the files on their hard drive, send e-mail and instant messages, shop online, and even engage in social networking through Google. In all, Google has amassed an extensive web search information infrastructure comprising nine distinct information-seeking contexts: general information inquiries, academic research, news and political information, communication and social networking, personal data management, financial data management, shopping and product research, computer file management, and Internet browsing.<sup>5</sup> Inherent in this infrastructure is the ability to collect and aggregate a wide array of personal and intellectual information about its users (see Table 1).

---

<sup>5</sup> These nine contexts are not necessarily mutually exclusive and are not put forth as airtight metaphysical divisions. They are meant simply to help compartmentalize the various types of information-seeking activities a person undertakes in her daily activities for easier discussion.

By striving to “organize the world’s information and make it universally accessible and useful” and create the perfect search engine, Google has assembled over two dozen interconnected products and services within their growing information infrastructure. Google’s encouragement of the creation of Google Accounts, combined with its use of persistent web cookies, provides the necessary architecture for the creation of detailed server logs of user’s browsing history both on Google web properties and beyond. The result is an infrastructure of dataveillance, arming Google with the ability to collect and aggregate a wide array of personal and intellectual information about its users, extending beyond just what website they search for, but also including what news they read, what interests they have, the blogs they follow, the books they enjoy, the stocks in their portfolio, and perhaps even every website they visit.

### Discussion

It is easy to think of search engines like Google as one-way information interfaces: you enter a search term, and you get results. You click on a link, and they direct you to a website, a helpful map, or a news report. But there is an important feedback loop; the interface is two-way. More than just the center of gravity of information seeking online, Google’s information infrastructure also acts as a black hole, using its gravitational forces to pull as much information about its users *into* its domain as possible. By monitoring and aggregating the results of every web search performed, every image result clicked, every website bookmarked, or every page visited with the Toolbar, Google has created sophisticated infrastructure of dataveillance. The result is what John Battelle calls a “database of intentions”:

This information represents, in aggregate form, a place holder for the intentions of humankind - a massive database of desires, needs, wants, and likes that can be discovered, subpoenaed, archived, tracked, and exploited to all sorts of ends. Such a beast has never before existed in the history of culture, but is almost guaranteed to grow

exponentially from this day forward. This artifact can tell us extraordinary things about who we are and what we want as a culture. (Battelle, 2003)

While many of our day-to-day habits – such as using credit cards, ATMs, cell phones, or automated toll collection systems – leave countless “virtual footprints” of our activities, the panoptic gaze of Google’s infrastructure of dataveillance tracks our search histories, e-mails, blog posts or general browsing habits, providing “an excellent source of insight into what someone is *thinking*, not just what that person is doing” (Hinman, 2005, p. 23).

The full effects of the panoptic gaze of Google’s infrastructure of dataveillance are difficult to predict. Clive Norris warns of how such infrastructures could be used to “[render] visualization meaningful for the basis of disciplinary social control” (Norris, 2002, p. 251). Instances of how users of Google’s infrastructure were made visible for the exercise of disciplinary power include a court ordering Google to provide the complete contents of a user’s Gmail account, including e-mail messages he thought were deleted (McCullagh, 2006) and the introduction of evidence that a suspected murderer performed a Google search for the words “neck snap break” (Cohen, 2005). While Google appears to recognize, at least partially, the disciplinary threat of storing such robust records of its users activities when it announced it would move user data collected from its Chinese site outside of the country in order to prevent China’s government from being able to access the data without Google’s consent (McMillan, 2006), the company recently agreed to comply with a Brazilian court order to release data on users of its Orkut social networking site to help Brazilian authorities investigate use of the site related to racism, pedophilia and homophobia (Downie, 2006).

Google’s infrastructure of dataveillance also spawns instances of “panoptic sorting” where users of Google are identified, assessed and classified “to coordinate and control their access to the goods and services that define life in the modern capitalist economy” (Gandy, 1993,

p. 15). Google, like most for-profit search engine providers, is financially motivated collect as much information as possible about each user: receiving personalized search results might contribute to a user's allegiance to a particular search engine service, increasing exposure to that site's advertising partners as well as improving chances the user would use fee-based services. Similarly, search engines can charge higher advertising rates when ads are accurately placed before the eyes of users with relevant needs and interests (Hansell, 2005). Through the panoptic gaze of its diverse suite of products, Google collects as much information as possible about an individual's behavior, and considers it to be potentially useful in the profiling and categorization of a user's potential economic value: recognizing that targeted advertising will be the "growth engine of Google for a very long time", Google CEO Eric Schmidt stressed the importance of collecting user information, acknowledging that "Google knows a lot about the person surfing, especially if they have used personal search or logged into a service such as Gmail" (Miller, 2006).

Perhaps the most potent consequence of the panoptic gaze of Google's infrastructure of dataveillance is how, like Bentham's original Panopticon, it might induce "a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault, 1977, p. 197). The rising anxiety among searchers about the presence of such systematic monitoring of their online information-seeking activities (Barbaro & Zeller Jr, 2006; Hafner, 2006; Levy, 2006; Maney, 2006), coupled with the rapid emergence of various tools and strategies to help hide or obfuscate one's web search activity from being easily tracked and monitored (Howe & Nissenbaum, 2006; Schoen, 2006; Singel, 2006) reveals a growing awareness of the effects of Google's panoptic gaze. Yet, the adoption rates of such tools remains unknown, and as Google

continues to expand its information infrastructure,<sup>6</sup> it becomes arduous for everyday users to recognize the data collection threats of these services, and easier to take the design Google's infrastructure of dataveillance merely "at interface value" (Turkle, 1995, p. 103).

By amassing a tantalizing collection of, admittedly, innovative and useful tools, coupled with requiring the divulgence of personal information as a precondition for using many of their new information and communication technologies, Google has constructed an information-seeking environment whereby which individuals are continuously integrated into a larger infrastructure of dataveillance. Greg Elmer warns of the dangers of such an environment where the collection of personal information is a prerequisite of participation inevitably entrenches power in the hands of the technology designers:

Ultimately, what both requesting and requiring personal information highlight is the centrality of producing, updating, and deploying consumer *profiles* – simulations or pictures of consumer likes, dislikes, and behaviors that are automated within the process of consuming goods, services, or media and that increasingly anticipate our future needs and wants based on our aggregated past choices and behaviors. And although Foucault warns of the self-disciplinary model of punishment in panoptic surveillance, computer profiling, conversely, oscillates between seemingly rewarding participation and punishing attempts to elect not to divulge personal information. (Elmer, 2004, pp. 5-6)

This blurring of punishments and rewards – subtle *requests* and not so subtle *commands* for personal information – reoccurs in Google's information interface where the default settings and arrangement of services make the collection of personal information automatic and difficult to resist.

In conclusion, the continued sophistication and expansion of search engine practices – epitomized by Google's suite of information-seeking products – represent the emergence of a new "social, political, and technical infrastructure that renders visualization meaningful for the

---

<sup>6</sup> Recent additions to Google's product suite include web-based word processor and spreadsheet services, enterprise solutions for business use, online digital photo sharing, website authoring tools, and an online database package.

basis of disciplinary social control” (Norris, 2002, p. 251), whose “methodical, technology-driven, [and] impersonal” panoptic gaze is quickly becoming “a primary mechanism of surveillance and, by extension, social control in our society” (Staples, 2000, p. 5). These search-based infrastructures of dataveillance increasingly contribute to a rapidly emerging “soft cage” (Parenti, 2003) of everyday surveillance, where they, like other dataveillance technologies before them, contribute to the curtailing of individual freedom (Solove, 2004, p. 33), affect users’ sense of freedom and concept of self (Morgan & Pritchard, 2005, p. 119), and present issues of “deep discrimination...and social justice” (Lyon, 2003b, p. 1).

Table 1: Google Suite of Products and Services

| <b>Product</b>                                | <b>Description</b>  | <b>Information Collected</b>  | <b>Notes</b>   |
|---|---|---|--|
| <i>1. General Information Inquiries</i>       |   |   |  |
| Web search                                    | Query-based website searches                                  | <ul style="list-style-type: none"> <li>• Web search queries</li> <li>• Results clicked</li> </ul>   |  |
| Personalized Homepage                         | Customized Google start page with content-specific modules    | <ul style="list-style-type: none"> <li>• News preferences</li> <li>• Special interests</li> <li>• Zip code</li> </ul>   | <ul style="list-style-type: none"> <li>• Use in conjunction with Google Account is encouraged</li> </ul>   |
| Alerts  | E-mail alerts of new Google results for specific search terms | <ul style="list-style-type: none"> <li>• News preferences</li> <li>• Special interests</li> <li>• E-mail address</li> </ul>   | <ul style="list-style-type: none"> <li>• Alerts for a user's own name (vanity search) are common</li> </ul>  |
| Image Search                                  | Query based search for website images                         | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Results clicked</li> </ul>   |  |
| Video   | Query based search for videos hosted by Google                | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Videos watched/downloaded</li> <li>• Credit card information for purchased videos</li> <li>• E-mail details for shared videos</li> </ul> | <ul style="list-style-type: none"> <li>• Google Video Player available for download with additional DRM technology</li> </ul>  |
| Book Search                                   | Full text searches of books scanned into Google's servers     | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Results clicked</li> <li>• Pages read</li> <li>• Bookseller pages viewed</li> </ul>  | <ul style="list-style-type: none"> <li>• Google Account required in order to limit the number of pages a particular user can view</li> </ul>   |
| <i>2. Academic Research</i>                   |   |   |  |
| Scholar                                       | Full text searches of scholarly books and journals            | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Results clicked</li> <li>• Home library (Optional)</li> </ul>  |  |
| <i>3. News and Political Information</i>      |   |   |  |
| News  | Full text search of recent news articles                      | <ul style="list-style-type: none"> <li>• News search queries</li> <li>• Results clicked</li> </ul>  | <ul style="list-style-type: none"> <li>• With a Google Account, users can create customized keyword-based news sections</li> </ul>   |
| Reader  | Web-based news feed reader                                    | <ul style="list-style-type: none"> <li>• Feed subscriptions</li> <li>• Usage statistics</li> </ul>  |  |
| Blog Search                                   | Full text search of blog content                              | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Results clicked</li> </ul>   |  |
| <i>4. Communication and Social Networking</i> |   |   |  |
| Gmail   | Free web based e-mail service with contextual advertising     | <ul style="list-style-type: none"> <li>• Text of email messages</li> <li>• E-mail searches performed</li> <li>• Email address or cellphone number (used for account creation)</li> </ul>                    | <ul style="list-style-type: none"> <li>• Creation of GMail account automatically results in activation of Google Account</li> <li>• Logging into Gmail also logs user into their Google Account</li> </ul> |

|   |  |   |  |
|---|--|---|--|
| Groups                                  | Free web based discussion forums   | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• User interests</li> <li>• Usage statistics</li> <li>• Profile information</li> </ul>   | <ul style="list-style-type: none"> <li>• Includes complete Usenet archives dating back to 1981</li> <li>• Google Account required for creation of new Group; User encouraged to create detailed profiles, including name, location, industry, homepage, etc</li> </ul> |
| Talk                                    | Web-based instant messaging and voice calling service  | <ul style="list-style-type: none"> <li>• Contact list</li> <li>• Chat messages</li> <li>• Usage statistics</li> </ul>   | <ul style="list-style-type: none"> <li>• Google Account and Gmail e-mail address required</li> </ul>   |
| Blogger                                 | Web-based blog publishing platform   | <ul style="list-style-type: none"> <li>• Weblog posts and comments</li> <li>• Profile information</li> <li>• Usage statistics</li> </ul>  | <ul style="list-style-type: none"> <li>• Google Account required</li> <li>• Users encouraged to create detailed profiles, including name, location, gender, birthday, etc</li> </ul>   |
| Orkut                                   | Web-based social networking service  | <ul style="list-style-type: none"> <li>• Profile information</li> <li>• Usage statistics</li> <li>• E-mail address and content of invitations</li> </ul>  | <ul style="list-style-type: none"> <li>• Invitation-only</li> <li>• Google Account required</li> <li>• Users encouraged to create detailed profiles, including name, location, gender, birthday, etc</li> </ul>  |
| Dodgeball                               | Location-based social networking service for cellphones  | <ul style="list-style-type: none"> <li>• Profile information</li> <li>• E-mail address</li> <li>• Location</li> <li>• Mobile phone information</li> <li>• Text messages sent</li> </ul>                 | <ul style="list-style-type: none"> <li>• User location when messages sent are tracked by Google</li> </ul>   |
| <i>5. Personal Data Management</i>      |  |   |  |
| Calendar                                | Web-based time-management tool   | <ul style="list-style-type: none"> <li>• Profile information</li> <li>• Events</li> <li>• Usage statistics</li> </ul>   |  |
| <i>6. Financial Data Management</i>     |  |   |  |
| Finance                                 | Portal providing news and financial information about stocks, mutual funds; Ability to track one's financial portfolio | <ul style="list-style-type: none"> <li>• Financial quotes</li> <li>• Discussion group posts</li> <li>• Discussion group views</li> <li>• Portfolio (optional)</li> <li>• Profile information</li> </ul> | <ul style="list-style-type: none"> <li>• Google Account required for posting to discussion board</li> <li>• Names and e-mails are displayed with discussion posts</li> </ul>   |
| <i>7. Shopping and Product Research</i> |  |   |  |
| Catalog Search                          | Full text search of scanned product catalogs   | <ul style="list-style-type: none"> <li>• Product search queries</li> <li>• Results clicked</li> </ul>   |  |
| Froogle                                 | Full text search of online retailers   | <ul style="list-style-type: none"> <li>• Product search queries</li> <li>• Results clicked</li> <li>• Sites visited</li> <li>• Shopping list</li> </ul>   | <ul style="list-style-type: none"> <li>• Google Account required for shipping lists</li> </ul>   |

|                                    |   |  |  |
|------------------------------------|---|--|--|
| Local / Maps                       | Location specific web searching; digital mapping  | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Results clicked</li> <li>• Home location</li> </ul> | <ul style="list-style-type: none"> <li>• Search queries might include geographic-specific information</li> <li>• Default location stored via web cookie</li> </ul>   |
| <i>8. Computer File Management</i> |   |  |  |
| Desktop Search                     | Keyword based searching of computer files   | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Computer file index (Optional)</li> </ul>           | <ul style="list-style-type: none"> <li>• Search queries visible to Google under certain circumstances</li> <li>• Desktop file index is stored on Google's services if using Search Across Computers</li> </ul> |
| <i>9. Internet Browsing</i>        |   |  |  |
| Bookmarks                          | Online storage of website bookmarks   | <ul style="list-style-type: none"> <li>• Favorite websites</li> <li>• When visited</li> </ul>                          | <ul style="list-style-type: none"> <li>• Google Account required</li> </ul>  |
| Notebook                           | Browser tool for saving notes while visiting websites                                     | <ul style="list-style-type: none"> <li>• Notes and clippings</li> <li>• Sites annotated</li> </ul>                     | <ul style="list-style-type: none"> <li>• Google Account required</li> </ul>  |
| Toolbar                            | Browser tool providing access to various Google products without visiting Google websites | <ul style="list-style-type: none"> <li>• Search queries</li> <li>• Websites visited</li> </ul>                         | <ul style="list-style-type: none"> <li>• Use of some advanced features routes all browsing traffic through Google servers</li> <li>• Some features require Google Account</li> </ul>                           |
| Web Accelerator                    | Software to speed up page load times for faster web browsing                              | <ul style="list-style-type: none"> <li>• Websites visited</li> </ul>   | <ul style="list-style-type: none"> <li>• All browsing traffic is routed through Google servers</li> </ul>  |

## References

- Agre, P. (2003). Your Face is not a Bar Code: Arguments against Automatic Face Recognition in Public Places. Retrieved July 28, 2006, from <http://polaris.gseis.ucla.edu/pagre/bar-code.html>
- Andrews, P. (1999, February 7). The search for the perfect search engine. *The Seattle Times*, p. E1.
- Barbaro, M., & Zeller Jr, T. (2006, August 9). A Face Is Exposed for AOL Searcher No. 4417749. *The New York Times*, p. A1.
- Battelle, J. (2003, November 13). The Database of Intentions. *Searchblog*. Retrieved May 16, 2006, from <http://battellemedia.com/archives/000063.php>
- Battelle, J. (2004, September 8). Perfect search. *Searchblog*. Retrieved May 16, 2006, from <http://battellemedia.com/archives/000878.php>
- Bennett, C., Raab, C., & Regan, P. (2003). People and place: Patterns of individual identification within intelligent transport systems. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination*. (pp. 153-175). London: Routledge.
- Bennett, C. (1996). The Public Surveillance of Personal Data: A Cross-National Analysis. In D. Lyon, & E. Zureik (Eds.), *Computers, surveillance, and privacy*. (pp. 237-259). Minneapolis: University of Minnesota Press.
- Bennett, C. J. (2001). Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology*, 3(3)(3), 197-210.
- Bentham, J. (1995). *The Panopticon writings* (M. Bozovic, Trans.). London; New York: Verso.
- Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

- Brey, P. (2004). Ethical Aspects of Facial Recognition Systems in Public Places. *Journal of Information Communication and Ethics in Society*, 2, 97-109.
- Brin, S. & Page, L. (1998). The Anatomy of a Large-Scale Hypertextual Web Search Engine. *WWW7 / Computer Networks*, 30(1-7)(1-7), 107-117.
- Clark, H. (2006, August 23). Innovation: A waste of money? *Forbes.com*. Retrieved August 20, 2006, from [http://www.forbes.com/leadership/2006/08/23/leadership-innovation-requiredreading-cx\\_hc\\_0823moore.html](http://www.forbes.com/leadership/2006/08/23/leadership-innovation-requiredreading-cx_hc_0823moore.html)
- Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM*, 37(5)(5), 498-512.
- Cohen, A. (2005, November 28). What Google Should Roll Out Next: A Privacy Upgrade. *The New York Times*, p. A18.
- Cohen, J. (1996). A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace. *Connecticut Law Review*, 28(4)(4), 981-1039.
- Cohen, J. (2003). DRM and privacy. *Communications of the ACM*, 46(4)(4), 46-49.
- Diaz, A. (2005). *Through the Google goggles: Sociopolitical bias in search engine design*. Stanford University.
- Downie, A. (2006, September 8). Google carves a middle path on privacy. *The Christian Science Monitor*, p. 1.
- Electronic Privacy Information Center (1999, November 30). Internet Privacy. Retrieved July 28, 2006, from <http://www.epic.org/privacy/internet/default.html>
- Elmer, G. (2004). *Profiling machines: Mapping the personal information economy*. Cambridge, MA: MIT Press.

- Fallows, D. (2005). Search engine users: Internet searchers are confident, satisfied and trusting – but they are also unaware and naïve. *Pew Internet & American Life Project*. Retrieved October 15, 2005, from [http://www.pewinternet.org/pdfs/PIP\\_Searchengine\\_users.pdf](http://www.pewinternet.org/pdfs/PIP_Searchengine_users.pdf)
- Ferguson, C. (2005). That's next for Google? *Technology Review*, 108(1)(1), 38-46.
- Foucault, M. (1971). *The order of things: An archaeology of the human sciences*. New York: Vintage.
- Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans. [1st American ed.] ed.). New York: Vintage Books.
- Foucault, M. (1980). The Eye of Power. In C. Gordon (Ed.), *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*. (pp. 146-165). New York: Pantheon.
- Froomkin, A. M. (2000). The Death of Privacy. *Stanford Law Review*, 52(5)(5), 1461-1543.
- Gandy, O. (1993). *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview.
- Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century* (1st ed ed.). Sebastopol, CA: O'Reilly.
- Goldman, E. (2005). Deregulating Relevancy in Internet Trademark Law. *Emory Law Journal*, 54.
- Google. (1999, June 7). Google Receives \$25 Million in Equity Funding [Press Release]. *Google Press Center*. Retrieved August 18, 2006, from <http://www.google.com/press/pressrel/pressrelease1.html>
- Google. (2005a). Company overview. Retrieved May 3, 2006, from <http://www.google.com/corporate/index.html>

- Google. (2005b). Google Privacy FAQ. Retrieved May 3, 2006, from [http://www.google.com/privacy\\_faq.html](http://www.google.com/privacy_faq.html)
- Google. (2005c, October 14). Google Privacy Policy. Retrieved May 3, 2006, from <http://www.google.com/privacypolicy.html>
- Gussow, D. (1999, October 4). In search of. *St. Petersburg Times*, p. 13.
- Hafner, K. (2006, January 25). After subpoenas, Internet searches give some pause. *The New York Times*, pp. A1, A19.
- Hafner, K., & Richtel, M. (2006, January 20). Google resists U.S. subpoena of search data. *The New York Times*, pp. A1, C4.
- Hansell, S. (2005, September 26). Microsoft plans to sell search ads of its own. *The New York Times*, pp. C1, C8.
- Hansell, S. (2006, August 8). AOL Removes Search Data On Vast Group Of Web Users. *The New York Times*, p. C4.
- Hargittai, E. (2002). Beyond logs and surveys: In-depth measures of people's web use skills. *Journal of the American Society for Information Science and Technology*, 53(14)(14), 1239-1244.
- Hellweg, E. (2002, April 22). Google's need for speed. *CNN/Money*. Retrieved August 20, 2006, from <http://money.cnn.com/2002/04/22/technology/techinvestor/hellweg/index.htm>
- Hinman, L. (2005). Esse est indicato in Google: Ethical and political issues in search engines. *International Review of Information Ethics*, 3, 19-25.
- Ho, S. Y. (2005). An exploratory study of using a user remote tracker to examine web users' personality traits. *Proceedings of the 7th international conference on Electronic commerce*, 659-665.

- Horrigan, J., & Rainie, L. (2006, April 19). The Internet's Growing Role in Life's Major Moments. *Pew Internet & American Life Project*. Retrieved May 26, 2006, from [http://www.pewinternet.org/PPF/r/181/report\\_display.asp](http://www.pewinternet.org/PPF/r/181/report_display.asp)
- Howe, D., & Nissenbaum, H. (2006). TrackMeNot. Retrieved August 27, 2006, from <http://mrl.nyu.edu/~dhowe/TrackMeNot>
- Introna, L. & Nissenbaum, H. (2000). Shaping the Web: Why the Politics of Search Engines Matters. *The Information Society*, 16(3)(3), 169-185.
- Jansen, B. J., & Resnick, M. (2005). *Examining Searcher Perceptions of and Interactions with Sponsored Results*. Paper presented at the Workshop on Sponsored Search Auctions at ACM Conference on Electronic Commerce, Vancouver, BC.
- Jansen, B. J., Spink, A., & Saracevic, T. (2000). Real life, real users, and real needs: A study and analysis of user queries on the web. *Information Processing and Management*, 36(2)(2), 207-227.
- Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, 50(4)(4), 1193-1294.
- Kopytoff, V. (2004, March 30). Google tests souped-up Web searches. *San Francisco Chronicle*, p. C3.
- Kopytoff, V. (2006, January 24). Most Web users say Google should keep data private. *San Francisco Chronicle*, p. C3.
- Kristol, D. (2001). HTTP cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology (TOIT)*, 1(2)(2), 151-198.
- Kushmerick, N. (1998, February 23). The search engineers. *The Irish Times*, p. 10.
- Levy, S. (2006, January 30). Searching for Searches. *Newsweek*, p. 49.

- Lyon, D. (2001). *Surveillance society: Monitoring everyday life* (Issues in society). Philadelphia: Open University Press.
- Lyon, D. (2002). Editorial. Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix. *Surveillance & Society*, 1(1)(1), 1-7.
- Lyon, D. (2003b). Introduction. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination*. (pp. 1-9). London: Routledge.
- Lyon, D. (Ed.). (2003a). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. London: Routledge.
- Lyon, D., & Zureik, E. (1996). *Computers, surveillance, and privacy*. Minneapolis: University of Minnesota Press.
- Maney, K. (2006, August 9). AOL's data sketch sometimes scary picture of personalities searching Net. *USA Today*, p. 4B.
- Marable, L. (2003). False oracles: Consumer reaction to learning the truth about how search engines work: Results of an ethnographic study.  
<http://www.consumerwebwatch.org/news/searchengines/index.html>
- Mayer-Schönberger, V. (1997). The Internet and Privacy Legislation: Cookies for a Treat? *West Virginia Journal of Law and Technology*, 1(1)(1).
- McCullagh, D. (2006, March 17). Police blotter: Judge orders Gmail disclosure. *News.com*. Retrieved June 20, 2006, from  
[http://news.com.com/Police%20blotter%20Judge%20orders%20Gmail%20disclosure/2100-1047\\_3-6050295.html](http://news.com.com/Police%20blotter%20Judge%20orders%20Gmail%20disclosure/2100-1047_3-6050295.html)
- McGann, R. (2005, March 14). Study: Consumers Delete Cookies at Surprising Rate. *ClickZ News*. Retrieved May 15, 2006, from <http://www.clickz.com/news/article.php/3489636>

- McMillan, R. (2006, March 1). Google moving search records out of China. *InfoWorld*. Retrieved August 20, 2006, from [http://www.infoworld.com/article/06/03/01/75996\\_030106HNgooglechina\\_1.html](http://www.infoworld.com/article/06/03/01/75996_030106HNgooglechina_1.html)
- McNamee, R. (2005, February 7). Google's Desktop Search. *The New Normal*. Retrieved May 2, 2006, from [http://thenewnormal.com/index.php/newnormal/googles\\_desktop\\_search/](http://thenewnormal.com/index.php/newnormal/googles_desktop_search/)
- Miller, M. (2006, March 17). Google's Schmidt Clears The Air. *PCMag.com*. Retrieved March 17, 2006, from <http://www.pcmag.com/article2/0,1895,1939257,00.asp>
- Mindlin, A. (2006, May 15). The Case of the Disappearing Cookies. *The New York Times*, p. C5.
- Mintz, H. (2006, January 16). Feds after Google data: Records sought in U.S. quest to revive porn law. *San Jose Mercury News*. Retrieved January 19, 2006, from <http://www.siliconvalley.com/mld/siliconvalley/13657386.htm>
- Morgan, N. & Pritchard, A. (2005). Security and social 'sorting': Traversing the surveillance-tourism dialectic. *Tourist Studies*, 5(2)(2), 115-132.
- Nagenborg, M. (2005). The ethics of search engines (Special issue). *International Review of Information Ethics*. 3
- Nielsen//NetRatings. (2006, August 21). Nielsen/Netratings Announces July U.S. Search Share Rankings. Retrieved August 21, 2006, from [http://www.nielsen-netratings.com/pr/pr\\_060821.pdf](http://www.nielsen-netratings.com/pr/pr_060821.pdf)
- Norris, C. (2002). From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control. In D. Lyon (Ed.), *Surveillance as Social Sorting*. (pp. 249-281). London: Routledge.
- Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: the rise of CCTV*. Oxford: Berg.

- Page, L., Brin, S., Motwani, R., & Winograd, T. (1998). The pagerank citation ranking: Bringing order to the web. Technical report. Stanford University, Stanford, CA.
- Parenti, C. (2003). *The soft cage: Surveillance in America from slavery to the war on terror*. New York: Basic Books.
- Pitkow, J., Schütze, H., Cass, T., Turnbull, D., Edmonds, A., & Adar, E. (2002). Personalized search. *Communications of the ACM*, 45(9)(9), 50-55.
- Rainie, L. (November 2005). Search engine use shoots up in the past year and edges towards e-mail as the primary Internet application. *Pew Internet and American Life Project*.
- Ramasastri, A. (2005, May 12). Can We Stop Zabasearch -- and Similar Personal Information Search Engines?: When Data Democratization Verges on Privacy Invasion. *FindLaw*. Retrieved June 12, 2006, from <http://writ.news.findlaw.com/ramasastri/20050512.html>
- Regan, P. (2001). *From Clipper to Carnivore: Balancing Privacy, Law Enforcement and Industry Interests*. Paper presented at the American Political Science Association, San Francisco, CA.
- Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill: University of North Carolina Press.
- Schoen, S. (2006, August 15). How To Keep Your Search History Private. *Electronic Frontier Foundation*. Retrieved August 15, 2006, from <http://www.eff.org/deeplinks/archives/004868.php>
- Schwartz, J. (2001, September 4). Giving the Web a Memory Costs Its Users Privacy. *The New York Times*, p. A1.

- Singel, R. (2006, January 20). How to Foil Search Engine Snoops. *Wired News*. Retrieved January 22, 2006, from [http://wired.com/news/technology/0,70051-0.html?tw=wn\\_tophead\\_2](http://wired.com/news/technology/0,70051-0.html?tw=wn_tophead_2)
- Solove, D. (2004). *The digital person: Technology and privacy in the information age* (Ex machina). New York: New York University Press.
- Stalder, F., & Lyon, D. (2003). Electronic identity cards and social classification. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination*. (pp. 77-93). London: Routledge.
- Staples, W. G. (2000). *Everyday surveillance: Vigilance and visibility in postmodern life*. Lanham, MD: Rowman & Littlefield.
- Suchman, L. (1997). Do categories have politics? The language/action perspective reconsidered. In B. Friedman (Ed.), *Human values and the design of computer technology*. (pp. 91-105). Cambridge, UK: Cambridge University Press.
- Sullivan, D. (2006, August 23). Hitwise Search Engine Ratings. *SearchEngineWatch*. Retrieved August 23, 2006, from <http://searchenginewatch.com/showPage.html?page=3099931>
- Swidey, N. (2003, February 2). A nation of voyeurs: How the Internet search engine Google is changing what we can find out about one another - and raising questions about whether we should. *The Boston Globe Sunday Magazine*, p. 10.
- Tavani, H. T. (2005). Search engines, personal information and the problem of privacy in public. *International Review of Information Ethics*, 3, 39-45.
- Tec-Ed. (1999, December). Assessing Web Site Usability from Server Log Files [White Paper]. Retrieved April 3, 2006, from [www.teced.com/PDFs/whitepap.pdf](http://www.teced.com/PDFs/whitepap.pdf)

- Teevan, J., Dumais, S. T., & Horvitz, E. (2005). Personalizing search via automated analysis of interests and activities. *Proceedings of the 28th annual international ACM SIGIR conference on Research and development in information retrieval*, 449-456.
- Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York: Simon & Schuster.
- Van Couvering, E. (2004). New media? The political economy of Internet search engines. *Annual Conference of the International Association of Media & Communications Researchers, Porto Alegre, Brazil*, 7-14.
- Ventura, H. E., Miller, J. M., & Deflem, M. (2005). Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power. *Critical Criminology*, 13(1)(1), 55-70.
- Ward, C. (1998, May 3). Grocery store shopper cards save money but cost privacy. *Houston Chronicle*. Retrieved August 20, 2006, from <http://www.chron.com/content/chronicle/business/98/05/03/grocerycards.1-1.html>
- Wouters, J. (2004, November 8). Searching for disclosure: How search engines alert consumers to the presence of advertising in search results. Retrieved Sept. 15, 2005, from <http://www.consumerwebwatch.org/news/paidsearch/finalreport.pdf>
- Zetter, K. (2005, May 17). Tor Torches Online Tracking. *Wired News*. Retrieved May 28, 2006, from <http://www.wired.com/news/privacy/0,1848,67542,00.html>
- Zimmer, M. (2005). Surveillance, privacy and the ethics of vehicle safety communication technologies. *Ethics and Information Technology*, 7(4)(4), 201-210.

Zimmer, M. (2006, January). The value implications of the practice of paid search. *Bulletin of the American Society for Information Science and Technology*. Retrieved April 3, 2006, from <http://www.asis.org/Bulletin/Dec-05/zimmer.html>