The Customer Commodity: An Analysis of Power Relations Between Companies and Consumers

Lucie Ferguson

As individuals participating in society, we leave trails of data regarding our actions, personal information, and histories wherever we go. This information is highly valuable to people wishing to target us for various purposes. In order to know as much about us as possible, they must seek out methods of collecting information from the paths we leave behind. The primary tool of doing this is surveillance.

As defined in The New Politics of Surveillance and Visibility, surveillance is "the collection and analysis of information about populations in order to govern their lives" (Haggerty & Ericson, 2006, p. 3). The definition can be adapted to apply to consumer surveillance in particular. Customers are a vast population; information about them is collected and analyzed by companies in order to govern what they consume, when and where they consume it, how they pay for what they consume, and nearly every other aspect of consumption. Ultimately, this leads to profit for the companies that are able to control the most. As scholar David Lyon (1994) pointed out, "the commercial data industry itself is worth fifty billion dollars a year in the USA" (p. 141). This number has likely increased in the past 13 years as companies continue to attempt to pull in patrons, showing that consumer surveillance has become even more integral to our capitalist society. Lyon indicated that society has always been information-based, but that personal information has recently been drawn into the market and become a commodity. Companies now trade consumer information databanks in order to cover the widest audience possible. Each name on a list of personal information has a price.

In his book "Profiling Machines," scholar Greg Elmer (2004) added that the more active pursuit of customer information has "been driven in part by obvious shifts in demographics, tastes and trends and in part by a rethinking of the nature of the consumer market itself, which seems to mark a shift in contemporary marketing culture" (p. 54). In other words, the growth in the consumer market leads to a change in the methods of consumer surveillance. Companies have to keep up with individuals' values in order to get the largest clientele possible. In addition, the "rethinking" of the consumer market means that customers have become a commodity, just as Lyon pointed out.

How aware are we of the degree to which we are being watched as consumers, and how does the sorting of our personal information affect our lives? Surveillance itself is not a new phenomenon, but with the rise of electronic technology, there are new issues regarding consumer privacy and awareness of when data is being collected as well as how it is being used. The recently increased capacity for storing and sorting information with computer databases makes it possible for huge amounts of data to be amassed and categorized easily. This systematic use of "banks" of personal information is known as dataveillance (Elmer, 2003, p. 235). It includes records of interactions and exchanges by customers, as well as addresses, credit histories, and any movements that can be recorded. Of course, there is potential for mistakes in this wide swath of collected information, and this can lead to repercussions for consumers, as we will see later in this paper.

This paper uses an ideological approach. Ideology deals with how a particular group uses knowledge to gain and keep power and how this affects society. In terms of consumer surveillance, ideological analysis helps us look at the way that businesses amass information about their customers and use this data in their own interests to keep control over the population

(Berger, 2000, p. 71). It allows observation of how companies' knowledge makes the relationship between consumers and sellers remain as it is and keeps consumers from being able to change it. As consumers, our only opportunity to escape from the ideological bindings of corporate power is to become informed about how and when we are surveyed.

To cover the topic fully, four questions will be addressed in this paper. Firstly, what is consumer surveillance? The answer to this includes groupings of the types of surveillance used by companies. We will see how some methods are based on a reward and punishment system, while others simply attempt to go unseen in order to ensure participation in the observation. Next, the paper will question the positive sides to surveillance methods, since much of the rest of the paper deals with negative aspects of consumer surveillance. While we are primarily looking at the ideological relationship between companies and the public, it is also important to analyze any perceived benefits to the collection of personal information. The third question deals with what comes after the actual surveillance of consumers. What is done with our information once companies have compiled it, and what implications does this have? Finally, how and why do companies maintain power over us as consumers? The model of the panopticon, a physical structure built for surveillance, will be used to discuss the power relations of consumer surveillance. These four questions will allow us to take a complete look at consumer surveillance and how we fit into the picture as consumers concerned with our privacy and rights. We will start with the basic understanding of what consumer surveillance means.

What is consumer surveillance?

As stated previously, consumer surveillance is any type of surveillance that observes the movement and information of consumers, whether they are people that have purchased before or are potential customers. The variety of consumer data types and surveillance methods is huge,

straddling anything from governmental census information to video and audio recordings of customers in department stores. In addition, different pieces of personal information gathered from surveillance are pieced together to form a more complete profile of each customer. Each profile belongs to various "niches," or groups whose information is valuable to advertisers looking for new customers to target or better ways to target old customers.

Today much of the surveillance of customers is performed with the aid of electronic devices and the Internet. Surveillance methods are often hidden in order to gain the most accurate data. Corporations share the huge databases they have accrued with one another in order to sort the public into socioeconomic groups and maximize the way they market products. However, the history of close consumer observance started with things like focus groups and brand testing.

One text that gives us a more historical angle to consumer surveillance is James Rule's Private Lives and Public Surveillance (1974). Rule discussed an overall picture of the ways in which our lives are surveyed such as policing, licensing (particularly in terms of automobile drivers), insurance approval, credit rating, and banking. While this is not specific to consumer surveillance, it does provide information about surveillance methods and how they achieve success, which are topics that would interest companies looking to increase control over customers. Most importantly, Rule points out that success depends on making sure that "clients cannot easily escape measures of control based on [the most 'complete'] information" (p. 302). For example, consumers cannot avoid having personal information known if they want the monetary savings that a supermarket card offers. Another example used by Rule is credit/loans, which are necessary in order to buy a house or other large purchase and require the collection of the consumer's personal information (p. 177). If you want to live what is considered a "normal"

or convenient life, you must adhere to this system. Most people simply cannot afford to not let companies have their personal information. The law of inescapable surveillance is key to the entire study.

When we apply this principle to modern day technology, it holds even truer. Rule referred to situations where it is made inconvenient for the customer to avoid surveillance, but in the Internet age, surveillance is often hard to detect. Customers cannot escape surveillance if they do not know when it is occurring. In terms of the ideological implications, companies are able to have control because there is no way for the public to question their influence. In summary, the main change in recent times is that surveillance is more pervasive and harder to find.

For the sake of understanding methods of consumer surveillance, it will be categorized into two main types. The first type is surveillance that can be avoided. Generally, this follows a rewards and punishment system. If people fill out a survey or use a special brand's card, they get something back, such as saved money on products. Customers are enticed into the situation by being offered special goods and services. When people do not take part, they are punished by having to pay more money or not being able to use the service. In a subtler sense, consumers are rewarded for participating by familiarity and convenience. If people give out their credit card information to an online store, they don't have to do it again and future purchases will be easier. An environment is created where we can make transactions easily because the flow of information is so great. In addition, rewards sometimes turn into punishments. Giving out one's home address in order to get a free service might land a person with new junk mail and telemarketing. Once a person accepts one offer, the barrage of requests increases, because companies share their databases of clients.

With surveys and savings club cards, it can be hard for consumers to argue that they cannot control observation of their personal information. Enticement-based surveillance is often a matter of choice. The system of rewards and punishments seems unfair, but still legal, since the customer is simply giving in to marketers' ploys and participating in the surveillance actively. However, Elmer (2004) pointed out that:

> [W]hile this 'enticement' model helps to qualify the process of surveillance as ultimately an act of solicitation and exchange, it also downplays the degree to which such 'requests' for personal information are altogether automated… or realistically provide customers with viable options to decline the offer (p. 30).

His point is that companies can get away with claiming that their methods of surveillance are optional. However, in reality it is hard to consistently find and use other, non-surveying services, especially as more and more companies add surveying components to their marketing strategies. In addition, not every surveillance method is based on the reward and punishment model. Other types of consumer surveillance are hidden, instead of acting as lures, making consumers unaware that it is even happening and consequently unable to avoid scrutiny.

One example of this is the Anne Droid, created by Jerry Gutierrez, a mannequin repairman (Tsiantar, 1989, p. 44). The Anne Droid is a store mannequin featuring closed circuit video cameras in the eyes and an audio recording device in the nose. Though it was originally marketed to companies as a tool to cut down on shoplifting and burglary, some department stores now install the dolls to find out what customers say about products and how they view product displays when they are not aware of being watched (Noonan, 1994, p. 78). Many stores already use closed circuit television for monitoring and to avoid theft. Anne Droids are an extension of this type of surveillance, but a more covert version.

Other types of in-store surveillance include Chameleon, a micro-magnetic thread hidden on items that sends a frequency to the store when it passes through a detector and Telltag, a microchip sensor that works in much the same way (Tsiantar, 1989, p. 44). While often these are advertised as ways to prevent theft, they also let stores know when a customer wearing a previously purchased item from the same brand enters, so they can greet them and suggest other items. These radio frequency identification (from this point on RFID) methods are essentially more technologically advanced versions of the plastic bars often seen on labels. Soon, all items purchased will have RFIDS, leading to greater convenience in price identification but also greater control over what is known about the customer. The main difference is that there is an increased secretive element to newer RFIDs. More and more, customers do not realize that their purchases have tracking devices.

With companies and the government sharing and selling personal information databases, as well as "hard surveillance" methods such as cameras and RFIDs, it has become harder to know when a person is being surveyed. In addition, if a person does not know when they are being observed, it is hard for them to prevent or stop it, so there is an increased inability to control what is known about them and their purchasing habits. This leads to the greater power of companies and marketers over the masses of consumers.

Web bugs are one example of a less controllable surveillance method. By programming nearly invisible HTML elements into a website, a website can keep track of a visitor's "clickstream – the sequence of Web sites visited by the user over time" (Martin, Wu &Alsaid, 2003, p. 258). These are usually placed in websites, but could also be used in emails. Also called pixel tags, Web beacons, and clear GIFs, Web bugs are used to monitor website traffic, interests, and problems with the flow of the website design. Does this method of surveillance work?

Martin, Wu, and Alsaid's study listed that there was "a very strong correlation between bug presence and the presence of leading brand names on Web pages" (p. 259). These methods of monitoring are used both to run a website effectively as well as to profile individual identities by what websites they visit, what they enter in search engines, and even give their demographic information to marketing companies. Each piece of information is relatively useless by itself, but when a user's online movements, zip code, gender, and phone number are combined, companies begin to have a strong profile of each person that can help them make assumptions about others. One example of Web bugs being used is with search engines. As people use search engines like Google more often, they will begin to see that when they visit sites, the banner and popup advertisements that appear feature the very interests that they searched. This is surveillance and targeting methods linked at a very simple level, but it illustrates how the system is effective.

Even though they are frequently undetected by Internet users, Web bugs are completely legal. Again, as with the Anne Droids, users generally do not question the presence of such methods of surveillance, because they are unaware of their existence. Another example of a way in which consumers may be unsuspecting targets of surveillance is cell phone satellite positioning monitors. Surveillance is all around; it is just not always apparent. It is important to try to learn what these methods are so that we can have a greater awareness of where our personal information goes and can make our own decisions about whether we want it to be known.

While there are differences between the reward and punishment type and the hidden type of surveillance,, both adhere to the law of successful surveillance by making it difficult to stay away from data collectors. If people want to participate in what is considered normal life, they have to give in to being watched. In other words, "surveillance becomes the cost of engaging in

any number of desirable behaviors or participating in the institutions that make modern life possible" (Haggerty & Ericson, 2006, p. 12). In order to gain the convenience and comfort that companies can offer, consumers have to give them something back. The price that they pay is their privacy and control over their personal information.

This notion of convenience is one of the benefits to the tracking of consumers' movements. Another possible gain is personalization for the customer. Surveillance has both positive and negative sides to it, and it is crucial to look at both in order to understand how our society of surveillance methods operates.

What are the positive effects of consumer surveillance?

While the tendency is to be protective of personal information and concerned about the growing lack of privacy, there are also positive side effects to surveillance for customers, including individualized shopping experiences and ease in payment with credit cards and previous purchase records. In fact, the increased knowledge of stores about their customers can seem very appealing. Lyon (1994) suggested that:

> [C]onsumer surveillance… is of a piece with designer goods, customized services, and other advances that take us beyond the world of standardized, uniform products and the accompanying limits on consumer choice. Its enabling capacity seems unquestionably desirable (p. 140).

Here we see that while some customers may feel uncomfortable being placed into an identity regarding recommendations, others enjoy the personalization. As scholar Ashlee Humphreys says, "we have not a culture of paranoids, as in the Panopticon, but a culture of narcissists" (p. 304). This shows a side to consumer surveillance that could be construed as positive or helpful.

Instead of a fight to keep our personal information private, there is a relationship of trade: we give out our data in return for a specialized and individualized service.

The online store *Amazon.com* provides an excellent example of the extensive knowledge companies have about customer movement and how it is used to create a special shopping experience. The website keeps track of a customer's wish list as well as what they have browsed/purchased; the next time they visit the site, it offers suggestions about what else they might like based on similar customers. Humphreys (2006) described the *Amazon.com* system as "[chronicling] mainly past and present desires and purchases in the service of statistically predicting future desires and purchases" (p. 299). In addition, credit card and address information is automatically kept on record to provide purchasing ease for the next visit. *Amazon* differs from some companies in that it does not hide the fact that it knows everything you view. It is actually extolled as a virtue. When a user logs in, the main page reads, "Hello [user name], we have recommendations for you" (www.amazon.com, 2007). This makes it easy for the user to slip right into purchasing mode instead of having to sift through items that he is not interested in. In addition, he may learn about new products.

A similar feature is used on Apple Computer's *iTunes* program. The Ministore monitors each song that is listened to, then recommends other music the user might enjoy (Shenk, 2006, p. G6). Likely, Apple also uses the information collected in marketing schemes later on. Since the recommendations are based on collaborative filtering (which creates links in the database of customer interests) both examples benefit from more users. This is true of most consumer surveillance methods. The wider the audience is, the better and more specific the profiling will be.

Even though the main set up of *Amazon*'s tracking is used as a selling point, other aspects of it are not as widely advertised. An article in the *New Statesman* gave readers tips on how to avoid being overcharged on the site. Just as the site keeps tabs on what items are purchased, it observes which of the available copies of items are purchased. The author noted that, "when Amazon looks at your past spending pattern, and sees that you have not always gone for the lowest price, they will treat you as a poor searcher – a more inelastic customer – and make you a less attractive price offer" (Sutherland, 2006, p. 53). In order to get a less biased price, users must log out, clear their computers' cookies and search again, this time anonymously.

Of course, using *Amazon.com* or *iTunes* is a choice, and most customers enjoy the convenience that it offers. If they do not want their browsing to be observed or their personal information to be kept track of, they have the option of going to a bookstore and paying in cash.

Non-web-based stores can also create personalized experiences by keeping track of customers' past purchases. This can be done through RFIDs, as previously mentioned. A catalogue company might also sell its list of customer addresses to a similar brand because they know the customer has interest in that type of product. While this is often seen as a negative effect because it produces "junk mail," presumably it could be a benefit for people looking to find more of the same products.

Collaborative filtering is one example of how the data collected regarding customers' information is sorted. However, sorting is not always used to the benefit of the consumer. In the next section, the process of data sorting and its results will be described and analyzed.

<u>What is done with the personal information that is collected?</u>

Observation itself is only the first part of the whole consumer surveillance picture. The database must be sorted to determine its importance and to create profiles of the customers

involved. Once customer information is procured, "statistical digestion of data digitally culled from diverse sources provides data entrepreneurs with profiles of consumers as members of certain crudely defined social groupings" (Lyon, 1994, p. 155). Some of this grouping is based on credit ratings, which in their most basic sense measure a person's ability to consume. These take into account whether bills are paid on time, how many loans and credit cards they have taken out, and how much they buy. This gives companies a sense of safety in knowing who to encourage to buy their products and who are possibly a less safe investment. The sorting is not only done with a single collection of data, it goes beyond that as "the contents of various apparently unrelated databases are raided to pull together personal information regarding names, addresses, telephone numbers, incomes, and consumer preferences" (Lyon, 1994, p. 142). For instance, a company might divide geographic area into neighborhoods, then determine what the median incomes, main ethnicities, education levels, and consumption habits are for each of those neighborhoods. Based on these classifications they can decide which areas to target depending on what product or service they are marketing as well as what types of promotional tools are best suited for the area. Not only this, but companies can avoid areas that have lost them money in the past, making surveillance and sorting into a form of risk management.

Humphreys (2006) goes beyond purely economic sorting with the discussion of "identity politics," meaning the collection of niches of customers (p. 300). These niches could be created from anything that people identify themselves with, such as moral values, favorite hobbies, political biases, or family backgrounds. Sometimes the people associated with a niche feel they are on the outside, or are not part of the dominant culture. By learning about these identities through surveillance, marketers then target them in future campaigns. Every piece of information about a person defines them in some way. And the more links a database gains, the better it

becomes at targeting more specific identity groups. This is one reason why corporations spend so much money on surveillance. They cannot afford to isolate any group of potential customers, so they must learn about these niches in order to appeal to those specific values.

Even if some people do not find issue with the actual collection of their personal information, they may feel their privacy and individuality is lost when they are sorted into these types of customer bases. In the beginning to their anthology about surveillance as a whole, Kevin D. Haggerty and Richard V. Ericson (2006) point out that, "where privacy rights have traditionally concentrated on the moment when information is acquired, citizens today seem increasingly anxious about how their personal data are combined and integrated with other pieces of information, and how they are used" (p. 9). The act of being grouped with other potential customers seems to violate the feeling of individuality and even control. Instead of being a multi-faceted person, a consumer is reduced to what Haggerty and Ericson call a "data double," or the flow of information created by that individual (p. 4). In turn, consumers do not necessarily know what is being done with their data double, which means they are losing control of themselves. They become faceless consumers, and this can feel like a loss of privacy.

Though the methods of surveillance discussed in this paper have generally been tied to consumption, data collecting corporations have power over consumers in more aspects than simply encouraging purchases. Once a profile is built about a customer, this information can be passed on to other entities that have nothing to do with the original collection. For instance, the government can rely on information gleaned from these huge databases if they want to know what transactions a suspicious individual has been making, what their credit is like, or even what they are reading. As Sutherland (2006) listed in his article about *Amazon.com*, corporations are "building up what must be a highly revealing bank of information about the thinking classes –

who are always, in the eyes of the authorities, the dangerous classes" (p. 53). Information about purchases and credit history is not only used to target people to buy more, but also to figure out what kind of person they are. This can lead to some interesting discussions about what is considered dangerous or not "normal." In turn, the government supplies census information to corporations for their profiling databases, creating a symbiotic relationship of information sharing, which consumers have no control over.

The desire to be an individual rather than a member of an array of groups is just one of the many problems consumers have with surveillance and sorting. Another issue is the "guilty before you're tried" mentality that goes along with such automated forms of grouping. A consumer's role and identity is determined before they even enter a store or apply for a job. In themselves, surveillance practices may not seem particularly heinous, but what are the implications of this clustering, especially if the personal information is incorrect? There is concern that "their privacy may be violated or their choices limited if salespeople know in advance – or worse, think they know – their caller's socioeconomic position and geographical location" (Lyon, 1994, p. 149). If we want to look at how companies keep the upper hand in the ideological relationship of corporation and consumer, pre-sorting is a huge element. For instance, before a person even contacts a company for a loan, the company has already determined whether you are a "safe" person to lend to based on whether they have paid bills on time or are a big spender. In a sense, the company has authority over whether the customer will even enter a decision-making situation, much less have control over what they choose. Haggerty and Ericson (2006) list two ways that misinformation can be created: errors in data entry and errors in organizational decisions (p. 17). The first kind of mistake means that the basic information is inherently wrong, such as having an incorrect address associated with a name. The second type

means that a mistake was made during the sorting process. For instance, mistakenly targeting an individual because an automated sorting program claims they fit a certain role. In terms of the consumer arena, mistaken identities mean repercussions, like rejected loans, because of incorrect poor credit, or being sent piles of junk mail for unwanted items because of being associated with someone else's information. Errors or not, automated pre-sorting hampers a consumer's freedom to choose.

So, it is clear that companies feel they need to group consumers into socioeconomic classifications in order to market more specifically and reduce the risk of losing money. The last step of understanding surveillance of consumers is to look at the way companies ensure that they have control over the consumer population.

How and why do companies maintain power over us as consumers?

The panopticon is a model used to look at the ideological approach of consumer surveillance. In the panopticon, the party in control is the one who can see – literally or figuratively – everything that the population it is monitoring does. This is based on Jeremy Bentham's and then Michel Foucault's concept of a centrally planned structure in which a "guard" in the middle can observe what goes on in the rooms surrounding his watchtower (Elmer, 2003, p. 232). It was originally planned as a way to create discipline in prisons, schools, and other institutions. The theory is that the panopticon gives the most possible control for the person in authority in the center, since he can see everything that goes on while the prisoners can see nothing. When this model is used on consumer surveillance, marketers are the ones at the center of the panopticon and consequently the ones in power. The consumer is a prisoner based on "the marketer's ability to collect information, to survey customers, and to hold information about their preferences for indefinitely long periods for a variety of ends" (Humphreys, 2006, p.

297). Instead of actual walls and windows, the architecture of the consumer panopticon is made up of the tasks consumers must perform where it is difficult or impossible for them to avoid being observed and analyzed.

In his book examining the panopticon, Oscar Gandy (1993) described the panoptic sort's modern form, saying, "a similar discriminatory process that sorts individuals on the basis of their estimated value or worth has become even more important today and reaches into every aspect of individuals lives in their roles as citizens, employers and consumers" (p. 1). This quote illustrates how databases are linked to provide the most complete profile of a person possible. In order for the panopticon of the corporation and consumer to be most successful, it is important for the marketer to have information about each person so they can control each aspect of the way they consume: where, when and how, as well as what.

Gandy, among others, claims this process is an underpinning of capitalist society. The ability of companies to sell their products, services, and ideas relies on their knowledge of the consumer audience as well as their ability to then manipulate the same people. For a very simple example, if a company knows when a woman is pregnant, they can deliver a sample of baby diapers to her and know she will have interest in their product, creating a potential customer.

Clearly, the consumer version of the panopticon is not an actual architectural model of the panopticon, like a prison. The panopticon is set up by making it difficult for consumers to live outside of the surveillance of marketers. How is this done? Consumers are "both rewarded with a preset familiar world of images and commodities and punished by having to work at finding different and unfamiliar commodities if they attempt to opt out" (Elmer, 2004, p. 49). For example, the only way to buy items online (or in many catalogues) is to use a credit card, and that requires giving personal information to the company. The only way to avoid this is to not

buy things online. As a whole, when consumers use the Internet, they have no guarantee of privacy. Other examples of this can be found in the types of consumer surveillance section of this paper. They all include the creation of a convenient environment that is unpleasant or difficult to leave.

The actual panopticon works on the theory that prisoners will eventually become self-disciplined, since they do not know when they are being watched. If this is applied to the consumer-corporation model, it assumes that we will at some point stop questioning the constant surveillance of our transactions and personal information.

It is so easy to use the products and services that are readily offered, and in our capitalist society, consuming constantly becomes more efficient. However, in order to have that kind of efficiency and convenience, it is necessary for consumers to succumb to the surveillance and sorting that goes with it. Which is worth more? Is there a meeting ground where consumers are able to control how much is known about them? Companies using consumer surveillance methods work to assure that consumers cannot find this meeting ground, because being able to control the movement of personal information cuts down on their profit.

Though this paper has pointed out many ways in which surveillance of consumers has increased, it should be pointed out that there have also been consumer rights groups formed. Some of these organizations include the Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) and the Public Interest Advocacy Center (PIAC), both of which deal with consumer privacy concerns. CASPIAN specifically works to get rid of supermarket savings cards and RFID chips, calling them “Big Brother in your grocery cart” (www.nocards.org, 2004). PIAC covers a wider area by providing consumers with free legal and research services. Both organizations are non-profit ones, and both groups combat the ideological assumption of

companies being able to know so much about consumers and have control over future decisions made, or even what decision-making situations they will get into. Especially since personal information is a commodity that is traded for money, it seems unfair that consumers often have no control over who has it and how it is sorted. In addition to knowing about what consumer surveillance methods exist, it can be useful to know what resources are available have if you feel your privacy is being violated.

It seems the best strategy for consumers is to try to learn as much as they can about what surveillance methods companies are using and what is being done with their personal information. In the panopticon model, the prisoners are unable to see who is watching them, or even anything outside of their own cell. In order to break out of the consumer panopticon, it is necessary for us as consumers to become more informed about the circumstances of our imprisonment. When we know about the reward and punishment model, it becomes a little easier for gusto reject it if so desired. Learning about more covert surveillance methods such as Web bugs gives information on what situations involve surveillance. Once we uncover these types, it is important to know about profiling and pre-sorting so that we are aware of our value and identity as customers, as well as our place in corporate databases. Once we have ascertained these things, we can make the choice about whether surveillance of our consumption habits is beneficial or a barrier to our freedom and privacy.

Works Cited

Berger, A. A. (2000). *Media and Communication Research Methods*. Thousand Oaks, California: Sage Publications.

Dichter, E. (1960). *The Strategy of Desire*. Garden City, NY: Doubleday and Company, Inc.

Elmer, G. (2003). A diagram of panoptic surveillance. *New Media & Society*, 5(2), 231-247. Retrieved November 10, 2007 from EBSCO host database.

Elmer, G. (2004). *Profiling Machines*. Cambridge: Massachusetts Institute of Technology.

Gandy, O. H. (1993). *The Panoptic Sort: A political economy of personal information*. Boulder, Colorado: Westview Press, Inc.

Haggerty, K.D.,& Ericson, R.V. (Eds.). (2006). *The New Politics of Surveillance and Visibility*. Toronto: Univ. of Toronto Press.

Humphreys, A. (2006). The Consumer as Foucauldian "Object of Knowledge." *Social Science Computer Review*, 24(3), 296-309. Retrieved October 2, 2007 from EBSCO host database.

Lace, S. (Ed.). (2005). *The Glass Consumer: Life in a surveillance society*. Bristol, United Kingdom: The Policy Press.

Lyon, D. (1994). *The Electronic Eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

Martin, D., Wu, H. &Alsaid, A. (2003). Hidden Surveillance by Web Sites: Web bugs in contemporary use. *Communications of the ACM, 46*(12), 258-263. Retrieved November 10, 2007 from EBSCO database.

Noonan, P. (1994). Spy Dummies. *Omni*, *16*(9), 78. Retrieved December 9, 2007 from EBSCO host database.

Packard, V. (1957).*The Hidden Persuaders*. New York: David McKay Company, Inc.

Rule, J.B. (1974).*Private Lives and Public Surveillance*. New York: Schocken Books.

Sutherland, J. (2006, February 13). The American Scene. *New Statesman*, 53. Retrieved October 2, 2007 from EBSCO host database.

Tsiantar, D. (1989). Big Brother at the Mall. *Newsweek*, 44. Retrieved December 3, 2007 from EBSCOhost database.