Nickolas Shlosman
BDIC Junior Year Writing
Tue Thur 1:00
Unit Paper on Surveillance

In today's world, information is a form of currency that can separate a successful corporation from one not fit for growth in the modern competitive climate. The internet age and its digital platforms have allowed companies and organizations to collect consumer data on grand scales for marketing, gain, and profit. Now more than ever, information that many consider to be private is being widely collected and used by others without the knowing consent of internet users. Through various methods of hacking and tracking, corporations have developed ways of processing digital consumer behavior to strategically benefit business. But how is "private" information and behavior being accessed without consequence? Because the internet is a relatively new unregulated platform, concrete legislation has not caught up with the progression of the digital age to ensure privacy protection for consumers. This gap in regulation has opened doors for companies to collect and exploit digital user data. If a third-party organization had the desire to surveil an individual for information that would normally be difficult to find, they could do so using a number of common surveillance processes implemented on a regular basis by many onto many. Although this particular scenario is applied on grand scales on entire pools of consumers worldwide, analyzing it as an individual case will help us better understand the methods of data collection and its practical shortcomings before we acknowledge the ethical concerns that accompany the matter overall.

Relative to the creation of foundational privacy laws in the United States, the digital platforms available and used by people today are new and do not fall into the jurisdictions of

our outdated constitution. Although the principals lined out by these founding doctrines are vital to how we, as a country, function, modern arrivals such as the internet do not entirely apply to limits set by old legislation, and ultimately allow private online behavior to fall into the hands of others. In the business of consumer information, organizations use a number of tools and loopholes in the law to access "private" digital data for their advantage. A main force utilized by industries is marketing data companies known as *data brokers.* According to a report by *Cracked Labs* on *Corporate Surveillance in Everyday Life*, "a data broker can be defined as a *company or business unit that earns its primary revenue by supplying data or inferences about people gathered mainly from sources other than the data subjects themselves*" (Christl, 40). Through means that do not necessarily involve direct hacking, data brokers utilize analytics to prioritize current and prospective customers for client companies. With personalized marketing techniques varying anywhere from telemarketing scripts to ad content, companies can use the information collected by data brokers to efficiently retain customers and target potential consumers. In the report, Wolfie Christl sources the US Federal Trade Commission (FTC) to explain that massive amounts of data collected by data brokers is turned into individual profiles about consumers without their knowledge (40). The ability to personalize marketing efforts on mass scales without consenting knowledge is an important observation to take away from the practices of corporate surveillance, because it reveals a vast network of manipulation for nothing other than profit and power. Data broker companies are just one example of methods used by corporations to collect private user information, and because legislation has not caught up to the rapidly expanding frontier of the digital world, these methods of surveillance, although technically legal, are taking advantage of unaware users through effective and

profitable manipulation.

Although digital user data is a valuable currency in today's corporate world, differences in quality of the data itself offer insights into the practical shortcomings of online tracking. Profiles of consumers configured by data collection and processing can vary in value depending on the complexity of a consumer's profile. According to an article by *Share Lab* on Facebook user data, titled *Quantified Lives on Discount*, the quality of an individual's profile can be broken up into three categories. The least valuable data that can be collected is that of the *basic information* category, which includes location, age, gender and language. Next is *detailed targeting*, which is based on user demographics, interests, and behaviors. And the most valuable of the three categories is *connections*, which scales and identifies the specific kind of relation a user has to pages, apps, people, or events (Share Labs, 2016). If we return to our scenario, a company's pursuit of and individual's information can produce various results depending on the quality of profile configured. From the practical standpoint of the organization, the objective is to gain the most detailed picture of a consumer by configuring a user profile that not only includes basic information like age and gender, but also interests, behavior patterns, and levels of attachment to involvements online. If the information collected on the individual of interest is not of high quality, the configured profile of that individual is a shallow misrepresentation of the user. This digital blueprint serves as a distant virtual skeleton, void of intricacies that would otherwise be vital for companies in a consumer marketplace. Even if behavioral patterns and interests are factored into a collected profile, the algorithms responsible for sorting information are basing profile configurations solely on the clicking of a mouse rather than confirmed actions backed by intent. The practice of collecting online user

data, although highly valued and profitable for companies operating on grand scales, can often create misrepresentations and falsely constructed profile configurations on an individual basis.

In addition to an organization losing accurate comprehension of certain consumers, individuals whose online behavior is falsely portrayed can face trouble if such behavior is analyzed at the hands of authorities. Along with corporations utilizing data for marketing and profit, we must not forget that a massive portion of digital surveillance is operated by government security agencies, especially in the United States. After the tragic events of 9/11, the National Security Organization began its efforts to track the communications data of the US citizens for national safety reasons. Since then, the measures implemented by the NSA have drastically escalated in intrusiveness, highlighting major ethical concerns over the past two decades of online government surveillance. Access to individuals' online behavior and digital data has allowed US agencies such as the NSA to unreasonably track those whose privacy is meant to be valued by our foundational laws. In the book *Dragnet Nation*, author Julia Angwin describes the increasing commonality of "suspiciounless investigations" around 2008. Here, Angwin talks about new guidelines passed by the attorney general allowing the FBI "to launch investigations without *any particular factual prediction*" along with authorizations made in 2012 permitting "the National Counter-terrorism Center to copy entire government databases of information about U.S. citizens" to "examine the files for suspicious behavior" (Angwin, 27-28). Although these are just a couple of examples of how pervasive government tracking has become since 9/11, they reveal that reasonable causes for suspicion no longer apply to government practices. Actions taken by these security agencies are now on a platform of preemptive measure and ignore ethical concerns regarding the privacy of citizens. Due to a lack

of trust and protective legislation, corporations and government security agencies have taken advantage of digital surveillance power in the pursuit of profit and control, while ultimately breaking ethical boundaries pertaining to privacy and authoritative measures for consumers and citizens alike.

The rapid evolution of technology and digital platforms over the last thirty decades has turned consumer data into one of the most valuable assets for organizations worldwide. Through methods that bypass outdated privacy laws, both corporations and security organizations have been able to collect, process, and exploit data on grand scales for business growth and control. Even though these wide-reaching practices work as a whole to feed the massive corporate world, misrepresentations of individuals' online profiles create gaps between what is real and what is a shallow virtual portrayal. As a result, such shortcomings in representation have raised ethical dilemmas of truth, privacy, and trust, especially when sought out by government security agencies who have abused their investigatory powers since the initial safety concerns posed by 9/11 almost two decades ago. While the progress of technology has created unthinkable possibilities for the world, the opportunities that come with such a new digital age can be driven to excess if not for the consideration of the people involved. In order to avoid being thrown into the panoptical future envisioned by George Orwell, the unbalanced scale of lacking trust and abusive power must be tipped level with the aid of protective legislation and ethical standards on privacy, truth, and freedom.