

# Ethical Issues of Data Surveillance

*Joseph Donahue, Nicholas Whittemore, Ashley Heerman*

---

## **Introduction**

Data surveillance, also known as dataveillance, compiles personal information from various sources to investigate or monitor people's daily activities and interactions amongst each other. Data surveillance has proven to be far cheaper and more effective than traditional forms of surveillance and is quickly increasing in popularity throughout a number of different fields. "It has been around since the late 1980s, but its use has jumped significantly over the past few years thanks to the increasingly widespread concerns for individual privacy in the Internet age."<sup>1</sup> There is an assortment of different ways dataveillance can be used to observe and examine one's actions. Our everyday life has essentially turned into one giant paper trail. Between using savers' cards at the supermarket, credit cards for purchases, or even just browsing the Internet, these actions are tracked electronically in databases and create personal data profiles for everyone engaged in these daily activities. Profiles are then massed together and filtered through by various organizations that use them for varying purposes. Broadly speaking, many people are content with this to a certain extent when it relates to our nation's security; however, are we using this information in ways that are harming our society? The potential issues of both personal and mass dataveillance pose ethical dangers and need to be more closely regulated by both individuals and the government.

## **Personal & Mass Dataveillance**

There are two main types of dataveillance; mass data surveillance and personal data surveillance. Mass dataveillance refers to the surveillance of groups of people; where as personal dataveillance refers to the surveillance of one specific individual. It is our goal to prove these dataveillance practices pose ethical dangers and are unnecessary to the extent that they are being used.

### *Personal Dataveillance*

There is typically a reason for the initial investigatory practices in personal dataveillance. For example, corporations use it to discredit individuals to avoid hiring, justify firing, or other background research for an assortment of different reasons. The following are some of the different types of personal dataveillance.

Profiling has proven to be the most common form of dataveillance, though much about it is still unknown. Essentially, profiling is an advanced system of extreme stereotyping. As first defined and established by Roger Clarke, a data surveillance specialist from Canberra, Australia, “It is a means of generating suspects or prospects from within a large population, and involves inferring a set of characteristics of a particular class of person from past experience, then searching data-holdings for individuals with a close fit to that set of characteristics.”<sup>2</sup> We all use profiling in our day-to-day lives. Profiling in terms of dataveillance begins to become a problem when assumptions about someone are made based on religion, looks, race, or actions and used to inhibit their freedom.

Front-end verification and front-end audit are two additional extensions of how dataveillance can be used. Front-end verification is when data is collected that is directly relevant to the primary event. For instance, when applying for a credit card, the credit card company may search past payment records, and/or previous credit card companies to obtain history on the individual. If there are inconsistencies in the information they have on a credit report and information they have retrieved from outside sources, one might not be able to obtain a credit card at that time. The purpose of both front-end verification and front-end auditing is to find inconsistency among sources to potentially disqualify the person involved. The main difference is the extent of information retrieved. Front-end audit is when the information being obtained is not necessarily relevant to the primary event. The data is often found from alternate databases or from a third-party source. For example, when a bank is reviewing a car loan application, they may use this as an opportunity to search other past credit histories not directly pertaining to the car loan itself. It is often not clear whether the two sets of data are associated at all; many argue that they are not and this is an unethical practice because they are not related.

Cross system enforcement is “When the relationship of an individual to one organization is dependent on the relationship of the individual to another organization.”<sup>2</sup> For example,

students at the University of Colorado are unable to receive their diploma if they have unpaid campus parking tickets.

### *Mass Dataveillance*

“Mass dataveillance is concerned with groups of people and involves a generalized suspicion that some (as yet unidentified) members of the group may be of interest.”<sup>2</sup> Mass dataveillance is used in many of the same ways as personal dataveillance; such as *screening or authentication of transactions, front-end verification, and front-end audit*, but there is one important distinction. The way they differ for the masses as opposed to the individual is that mass dataveillance practices involve all transactions and individuals, “Whether or not they appear to be exceptional.”<sup>2</sup> This distinction holds true for all of the mass dataveillance techniques and poses ethical dangers to both individuals and our society.

It is important to understand the implications of the forms of surveillance imposed on American citizens. Many people are aware that such processes exist, but very few people have any idea to what extent their personal data trail affects their everyday lives. Organizations, like police departments, are using dataveillance in ways that pose serious threats to our society. Police detectives are “Encouraged by mass dataveillance to focus on minor offenses that can be dealt with efficiently, rather than more important crimes that are more difficult to solve.”<sup>2</sup> This poses serious threats to how impartial the law is perceived to be enforced, and creates a threat to the rule of the law. As dataveillance becomes more advanced and better known, “It will soon be possible to combine information from different sources to recreate individual’s activities with such detail that it becomes no different from being followed around with a video camera.”<sup>3</sup> Our goal is to address this ethical dilemma as it pertains to personal and mass dataveillance.

## **Dangers of Dataveillance**

### *The Effects of Personal Dataveillance*

There are currently a multitude of dangers regarding the continuing modernization of dataveillance. The first and most immediate of the threats is that there is not always an actual person monitoring the data. Often it is a computer system that is linking together pertinent facts to establish a conclusion. It is likely that a computer can commit errors and deliver information that is wrong and can potentially be overlooked because of the lack of personal monitoring. This

can pose a variety of other problems. An obvious example of this problem is wrongly identifying an individual into certain categories' based on his or her attributes and data trail. For instance, one might use his or her computer to purchase or research necessary items for a home project; this can lead them to be placed into a certain group of highly watched individuals if the items being looked at cross a certain key word (such as items that resemble pieces needed to make a home made bomb). If this scenario, or one similar to it happens, and an individual is wrongly identified, this can create a nightmare for someone trying to oppose false information.

A second problem is the quality of data. "For many organizations it is cost-effective to ensure high levels of accuracy of only particular items (such as invoice accounts), with broad internal controls designed to ensure a reasonable chance of detecting errors in less vital data."<sup>2</sup> There is currently no clear standard pertaining to the quality of data that needs to be in use in dataveillance systems. People often utilize the cheapest and easiest forms in order to keep costs down and information high, this is seen with the lack of regulations placed on dataveillance. Obviously, errors are a factor in low quality data, and an error in this field could jeopardize someone's livelihood. As stated earlier, this is specifically true in cases where people are not aware that their actions are being tracked and are unable to oppose the facts.

A third and equally important danger is the possibility of misinterpretation. Data is likely to be misinterpreted if all the pertinent facts are not taken into consideration. Dataveillance situations only involve the obvious, immediate facts. It is unlikely that a person, or a computer system, is going to do extensive research to make sure that the findings are correct based on the circumstances. "Technology used in online marketing has advanced to a state where collection, enhancement and aggregation of information are instantaneous. This proliferation of customer information focused technology brings with it a host of issues surrounding customer privacy."<sup>4</sup> An example of this is how Google.com is scanning users' websites and collecting data in order to better advertise to specific individuals. "The nature of the Internet requires information to flow two ways, placing Google in a position to collect vast databases of information describing who and how people use their services."<sup>5</sup> Most people are unaware that large, public companies such as Google are using dataveillance without individual's consent.

Currently, it is far more common for data to be collected without the individual's knowledge. If people are not aware they are being monitored, it is likely they are also unaware of the possibility that their information is being released to outside sources. Often data is released

and other organizations have access to it. This typically occurs because people usually do not read through consent forms about the release of information in its entirety. For example, in some states getting a marriage license is dependent on outstanding parking tickets through the city. How is it possible that they have access to that information? In most dataveillance situations, there is either a lack of the individual's knowledge of dataveillance or the lack of their consent to permit it. In recent years, this bubble of data that is being retained is leading to morally and ethically questionable procedures. In *front-end audit* and *cross systems enforcement*, it is possible for someone to be blacklisted from an organization or from obtaining something (a permit) based on an event that is not directly related. People are denied jobs because of certain diseases or past conditions, as well as denied insurance due to bad credit. In many cases, it is questionable if these factors are legitimate at all.

### *The Effects of Mass Dataveillance on the Individual*

As advancements and new technological improvements are made today, understanding the effects of new technologies on individuals' privacy and ways of life are significant. Data mining and dataveillance allow organizations to see what, when, where, and how you paid for purchases and categorize you based on them. Supermarket saver's cards and RFID or Radio-frequency identification tags are prime examples of this. Is this ethical? Organizations and large corporations are collecting large pools of data and grouping individuals based on a generalized suspicion. This poses ethical dangers because individuals can be falsely grouped based on routine procedures and actions. This can inhibit someone's chances to succeed in the work place or everyday life based on previous sporadic activities which can lead to misjudgments based on them. Information can tell you a lot about a person, but it does not paint a complete picture and is often taken out of its original context. As we have stated earlier, the techniques being used in dataveillance place individuals into certain groups and could pose some ethical dangers to individuals.

Mass data collection and surveillance will force you to look over your shoulder and see nothing, but know that there is someone, somewhere, collecting data; and in a sense, watching every move you make. These dangers are real and frightening. As individuals become placed into groups based on things they do, talk about and write about, they are being labeled without their knowledge. The individual needs to be aware of this. As the databases increase and become

easier to use and access, there needs to be boundaries to the information organizations can access.

### *The Effects of Mass Dataveillance on Society*

As explained above, mass dataveillance poses clear dangers to individuals, but what does this mean for our society as a whole? Is it ethical for companies to use mass dataveillance techniques that result in a prevailing climate of suspicion? What this means is that organizations that are using personal dataveillance “[normally investigate and monitor] after reasonable grounds for suspicion have arisen.”<sup>2</sup> On the contrary, when used, mass dataveillance is “routinely preformed and the suspicion arises from it.”<sup>2</sup> The right to privacy is not absolute, and in certain cases, it shouldn’t be. But what about those instances in which it should? As a society, should we accept that the explosive pace of technology advancement has a negative affect on our individual lives? Does the phrase “reasonable doubt” no longer hold any significance? Is it fair that organizations using mass dataveillance techniques can now come up with the information necessary to bring you down (i.e. fire you from your job) with no prior reasonable doubt? These are important questions that more people need to ask themselves as our technologies continue to advance.

Unfortunately, the rules and regulations that are being developed to combat some of these issues are being passed at a pace that is much slower than the pace at which the technology for further development of these data systems is expanding. In order for our society to combat the use of mass and personal dataveillance, we must become aware of how it is used, who uses it, and what they use it for. By becoming informed on these issues, we will have better means to avoid these techniques, or at the least, not become a victim of them.

### **Conclusion**

In closing, the increased use of dataveillance does not currently have any standards or regulations. The potential issues being described of both personal and mass dataveillance pose ethical dangers and need to be more closely regulated. It is not currently being monitored to the degree it should and we are still far from having laws governing the majority of these data surveillance techniques. It is being spread too fast and getting out of hand with the advancement of modern technology. It is vital that we begin to recognize and personally monitor our personal release of information. It is necessary to read and reread every document we are signing and ask

about the implications it could have. It is only when we begin to pay attention that we will be able to understand the incredible amount of information being held on each one of us. Then, hopefully, regulations will start to be imposed and we will have both privacy and freedom without compromising either.

## Works Cited

- [1] Paul McFedries Word Spy, June 13, 2001.  
<http://www.wordspy.com/words/dataveillance.asp>
- [2] Clarke, Roger. "Information Technology and Dataveillance." Roger Clarke's 'IT and Dataveillance' 1991. Xamax Consultancy Pty Ltd, Canberra. 7 Mar. 2007  
<<http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>>.
- [3] Stanley, Jay, and Barry Steinhardt. "Bigger Monster, Weaker Chains: the Growth of an American Surveillance Society." Jan. 2003. American Civil Liberties Union. 20 Mar. 2007  
<[http://www.aclu.org/FilesPDFs/aclu\\_report\\_bigger\\_monster\\_weaker\\_chains.pdf](http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf)>.
- [4] Laurence Ashworth, Clinton Free, " Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns," Journal of Business Ethics, June 13, 2001. <http://ssrn.com/abstract=889428>
- [5] Shaker, Lee. "Information Safety and Accuracy: is Google Trustable?" Robin Good. 15 May 2006. 10 Apr. 2007  
<[http://www.masternewmedia.org/news/2006/05/15/information\\_safety\\_and\\_accuracy\\_is.htm](http://www.masternewmedia.org/news/2006/05/15/information_safety_and_accuracy_is.htm)>.