Eric Holland
ECS188
5-21-04

Database Nation-The Death of Privacy in the 21st Century

Simpson Garfinkel paints an unappealing picture of our technological future and how we have given up our privacy with the advent of advanced technology. Garfinkel introduces concepts like “false data syndrome” and “data shadow” to help paint his picture. “False data syndrome” is when so much collected information is actually correct that we blindly accept when it is wrong without question and “data shadow” can be thought of as your digital trail. According to Garfinkel, “technology is not privacy neutral”. We only have two real choices: First) all our personal information must be allowed to fall under public domain or Second) we become hermits where we isolate ourselves from the world. Garfinkel’s thoroughly researched and example-rich text is a splash of cold reality and if we wish to see substantive changes for the better in our society, we need to make our voices heard, we need to demand our privacy and we need to demand it now (281).

Back in 1992, I got my first computer. It was a Packard Bell with 66Mhz and a small hard drive of 170MB. Now, only twelve years later from a company called LaCie you can purchase a hard drive with an amazing storage capacity of 1-Terabyte and it fits inside a manageable 5.25” form factor for a retail price

of $1000. To put the size of its storage capacity in perspective you can store two years of continuous music or one month of continuous MPEG-2 video. My point is that with increasing processor speeds and storage the quantity of information that can be stored about you or anyone else is reaching limitless proportions and with storage space at such a high, it never has to be deleted to make room for new information.

It’s not the United States government who controls or manages the majority of information but rather faceless corporations who trade your purchasing habits, social security numbers, and other personal information just like any other hot commodity. How do they get my information you ask? Everytime you use your credit card, ATM, or phone privacy is almost a nonexistent concept because your every move is being tracked and stored for future use. They know when, where, and what you purchased and for how much. Why? Telemarketing is big money. It is a trillion-dollar industry and it is growing all the time. On the internet every web page you visit, form you fill out, email you send is tracked so that a profile of your viewing habits can be determined to taylor advertisements just for you. You may be thinking…so what, if people really want to keep track of what I buy, what I view, or when I phone my mother then let them I have nothing to hide. Maybe you don’t mind getting junk

mail after all, it’s not that big of a deal I just toss it all in the trash you say. Okay, lets hit a little closer to home.

Most Americans would agree that their medical records are the most sensitive pieces of information they have (125). Doctors and medical institutions are required by state hosptial regulations to have a medical records department that ensures the confidentiality of patient records. A hospital or doctor can lose their accreditation if there is a pattern of confidentiality violation (126). Surprisingly however, there are few state or local laws that criminalize the unauthroized release of medical records themselves and no federal laws. Garfinkel sites many examples where individuals have lost their jobs and insurance because their medical records were released. Afterall, your insurance doesn’t want to insure you if you have a potentially deadly disease and an employer isn’t going to want to waste time and money training you to be a top executive if you might not be with the company in five to ten years. Insurance companies have you in a corner. They know you need insurance to get the medical treatment you so desperately need yet they make you sign away your right to privacy in order to get it. When you sign on the dotted line you agree that the insurance company can disclose any and all such information relating to your medical records. The problem is that this creates a dominoe effect in which all other insurance companies

can get your medical records. Before you know it, if you have a medical problem that makes you an insurance risk then you can't get insurance anywhere and if you somehow find an insurance company willing to take the risk, it is at a higher rate than normal. Did you know that according to the *Privacy Journal* compilation of state and federal privacy laws, only 23 states gives patients the right to view their own medical histories (141). There is definitely something wrong with the system when the government, corporations, and even employers can get a peek at your medical records but you can't. If nothing else, you have the right to correct any inaccuracies in your own medical records don't you? You'll all be glad to hear that California isn't one of them.

Let's shift gears and discuss how terrorism effects everyone's privacy. Terrorist tactics are changing. Old terrorists worked in large groups who used fear and violence for a cause. Today, they work in small groups sometimes even alone and not to invoke change but for revenge. New technologies have given terroists more deadly weapons such as recent anthrax scares. Terrorists can now kill entire city blocks unlike when a kook would go postal with a shotgun and kill just a handful. Since 9/11 security has increased not only in airports but also in office buildings and even the street with added police, security guards, and surveillance cameras. More security means

less privacy. We've all undergone or know someone who's had to deal with the new boarding policies at the airport. We all understand the need for security but some new policies under consideration threaten your privacy unlike any before. A universal smart card is being discussed as a new security measure. Your card would be linked to a central database that had everyone's information and I mean all your information. Information like tax records, medical records, school records, credit histories, legal records, etc. Using this information for security could provide airports potential threat levels of individuals. Threat levels would be color-coded. For example, lets use the colors green, yellow, and red. Green would indicate that there is nothing in a person's record that would lable him/her a threat. Yellow would indcate a more possible threat may exist and finally red would indicate that this person is more likely than anyone else to be a potential threat. There's talk that those who are green could board the plane without being subjected to the strictest security measures as opposed to those who are red who would face the strictest security measures. Who else might use such a smart card and for what? The problem with keeping databases of information is making sure that is is secure. We have all heard of identity theft and I'm really not sure if a central database is the answer or the way things are today where hundreds of different

databases have your information. Is it easier to secure one large database or hundreds of smaller ones? Even though security might be higher, if someone breaks into the one large database then they have access to all of your information and everyone else's. However, securing hundreds of databases might prove to be harder to implement. What do you think?

Privacy is at a crossroads. We have a say in how our privacy laws are made. Unfortunately, the U.S. doesn't have many laws on privacy and thus we need to be careful in how we shape it. A major frustration is that people aren't aware of current privacy laws and other possible solutions to protect their privacy. Not only do we need privacy laws for everyday circumstances but guidelines for technology as well. Privacy needs to be considered in the design element as well as in their use. A simple example is in webcams. Because it is cheaper to build a webcam without a shutter they often come without one. A simple yet effective means of privacy control would be to include a shutter so the user knows for certain that they aren't being recorded without their knowledge. I agree that this isn't a major privacy issue but the example demonstrates how privacy in current technology isn't considered to be a top priority.

Instead of creating a database nation, we need to create a future of freedom that honors personal autonomy and respects personal privacy. And we must start now (271).