CSE303, Spring 2005, Example "Issues" Paper

Note: The following "paper" is just an example of a reasonable submission for CSE303 (although it is a bit broader than ideal). As required, it provides background, takes a position, and defends that position. The purpose of this example is *not* to teach a particular opinion. As our class discussions have emphasized, the societal implications of computing are difficult and students should reach their own conclusions. It is simply impossible to give an example without expressing some (debatable) opinions.

Recent Digital Technology Endangers Personal Privacy
Dan Grossman
May 2005

We may have already reached an age of "constant surveillance" in the developed world, in which it is reasonable to assume that one's every action is recorded and available to anyone sufficiently interested in acquiring it. The enabling technologies (including ubiquitious communicating devices, tiny cameras, massive storage systems, and improved search techniques) have widely cherished uses, so we cannot and should not hope they disappear. Rather, if we value personal privacy (an ethical question well beyond this short essay), then we should develop data-management policies and legal requirements that allow individuals to control where their personal data is stored.

Modern technology lets us record a staggering amount of information about individuals' actions. Surveillance cameras in many buildings, tiny portable cameras in many pockets, and government satellites overhead enable image or video recording almost anywhere. Our networked computers, cable-television subscriptions, and credit cards allow service providers to learn our work and entertainment habits. Our communication devices make it easy to locate us whenever they are on and near us. In short, technology has made it unreasonable to assume our actions are visible only to those physically present at the time.

Continuing advances in digital storage capacity mean we can store all this information. The average home computer already has enough disk storage to store (with reasonable quality) the sound a person hears for her entire life. Corporate databases can include every item ever sold from a store or a trace of every visit to a website. There is simply no need to delete old data to make room for the new: For the reasonable future, we can expect to store everything more cheaply and in less physical space.

All this information is useless unless someone can find what they are looking for. Success in search technology, from the billions of successful web searches each day to cutting-edge data-mining techniques, suggests that we can often succeed in automating retrieval from our massive worldwide data collection. Searching images and video is more difficult than searching text, but nothing indicates the technical problems are insurmountable.

Together, ubiquitious digital recording and location-tracking, increased storage capacity, and sophisticated search create the ability to find any information about anything at anytime. This vision is appealing for many valuable uses such as replaying meetings (or sentimental

events), providing a worldwide information repository, and even advancing science and our understanding of human nature. But it also raises new ethical questions regarding who has the right to this data and what it can be used for.

Until humanity comes to understand the implications of technology relevant to personal privacy and reaches a consensus on its appropriate use, we should adopt a cautious strategy in which we affirm that each individual has the right to control information about herself. Corporations and governments should have to disclose the sort of information they store and individuals should have the right to have their information removed. Although this goal should guide our policies, several issues make it overly simplistic for a comprehensive solution.

First, aggregate information (such as averages and other statistics) are extremely useful and, at least potentially, disclose acceptably little information about individuals. It is unclear "how much aggregation is enough" and whether the "opt-out" strategy advocated above should affect aggregated results. If it does, opting out can introduce statistical bias. Databases of census information, disease outbreaks, even tax records serve a public good because they provide summary information that can guide public policy. Collecting this data accurately while ensuring privacy is a difficult balance.

Second, it is unclear how much privacy an individual should be allowed to forfeit voluntarily. Policies allowing one to maintain privacy are ineffective if every computer, software package, and financial account comes with a contract requiring the consumer to surrender their rights. Yet it is equally unreasonable to forbid any personal data collection. Tracking individuals' actions might lead to better service (e.g., phone-tower placement or identity-theft detection). With consenting participants, such activities are ethical and valuable.

Third, despite our ability to collect, store, and search massive amounts of information, we are likely not organized enough to enforce accurately any privacy policy. A fine-grained policy with each individual empowered to control data regarding her life would prove intractably complicated. Even an expert trained in technology and privacy issues would find it cumbersome to control such information. Without drastic simplification, the problem of controlling the deluge of personal information is just too difficult.

On the surface, the privacy issues that modern technology raises seem simple: As it becomes transcendingly easy to maintain personal information, personal privacy requires that individuals gain the ability to control the information about themselves. Doing so requires a delicate balance so that we neither ban data collection nor make it to difficult for someone who values privacy to protect their information. Today it seems our technology has outpaced our policies and ethical norms: We can collect the data, but it is not clear idea what bounds we should place on its use.