The ethics (or not) of massive government surveillance

CS201 Final Project by
Tony Wu
Justin Chung
James Yamat
Jessica Richman

The Ethics of Surveillance

Introduction to Surveillance

Surveillance is, simply put, the observation and/or monitoring of a person. Coming from the French word for "looking upon," the term encompasses not only visual observation but also the scrutiny of all behavior, speech, and actions. Prominent examples of surveillance include surveillance cameras, wiretaps, GPS tracking, and internet surveillance.

One-way observation is in some ways an expression of control. Just as having a stranger stare at you for an extended period of time can be uncomfortable and hostile, it is no different from being under constant surveillance, except that surveillance is often done surreptitiously and at the behest of some authority.

Todays technological capabilities take surveillance to new levels; no longer are spyglasses and "dropping" from the eaves of a roof necessary to observe individuals - the government can and does utilize methods to observe all the behavior and actions of people without the need for a spy to be physically present. Clearly, these advances in technology have a profound impact with regards to the ethics of placing individual under surveillance&emdash;in our modern society, where so many of our actions are observable, recorded, searchable, and traceable, close surveillance is much more intrusive than it has been in the past.

Surveillance and Physical Searches

Particularly interesting about government surveillance is that in the United States surveillance is not held to the same standards of accountability&emdash;as the Constitution protects American citizens from unreasonable searches and seizures, physical searches of individuals may not be conducted without a warrant issued by a judge. However, after the passage of FISA and subsequent laws, citizens have not been given the same protection with regards to electronic surveillance. As there have been massive changes in technology and lifestyle since the 1970s, electronic surveillance could be considered much more invasive than a physical search, yet as has been made clear in the legal section of this website, it is in fact much easier for government agents to perform surveillance. Why there is such disparity between these standards to us a matter of serious concern.

"If you haven't done anything wrong, you have nothing to fear."

This is a typical argument used by governments and other groups to justify their spying activities. Upon cursory inspection, it seems to make sense&emdash;as most people are law-abiding citizens, most ostensibly will not be targeted for surveillance and it will not impact their lives, while making their lives more comfortable and safer through the elimination of criminals. Thus, the government's use of closed-circuit television cameras in public spaces, warrantless wiretapping, and library record

checks have the potential to save lives from criminals and terrorists with only minimal invasion of its citizens' privacy.

First, as a mental exercise, we ask that the reader consider that these arguments could easily be applied to asking all citizens to carry location tracking devices&emdash;it would make tracing criminal acts much easier, and that it could easily be argued that people refusing to carry these devices only do so because they have something to hide. It is a matter of course that most people in our society would object to this solution, not because they wish to commit any wrongdoings, but because it is invasive and prone to abuse. Now consider that, given current technology, the government already has the ability to track a known target's movements to a reasonable degree, and has easy access to information such as one's purchasing habits, online activities, phone conversations, and mail. Though implementing mandatory location tracking devices for the whole population is certainly more invasive than the above, we argue that current practices are analogous, extreme, and equally unacceptable.

Next, this argument fails to take into consideration a number of important issues when collecting personally identifiable data or recordings&emdash;first, that such practices create an archive of information that is vulnerable to abuse by trusted insiders; one example emerged in September of 2007 when Benjamin Robinson, a special agent of the Department of Commerce, was indicted for using a government database called the Treasury Enforcement Communications System (TECS) for tracking the travel patterns of an ex-girlfriend and her family. Records show that he used the system illegally at least 163 times before he was caught (Mark 2007). With the expansion of surveillance, such abuses could become more numerous and more egregious as the amount of personal data collected increases.

In addition, allowing surreptitious surveillance of one form, even limited in scope and for a particular contingency, encourages government to expand such surveillance programs in the future. It is our view that the danger of a "slippery slope" scenario cannot be dismissed as paranoia - as a prominent example, the collection of biometric has expanded immensely in the past several years. Many schools in the UK collect fingerprints of children as young as six without parental consent (Doward 2006), and fingerprinting in American schools has been widespread since the mid-eighties (NYT National Desk 1983). Now, the discussion has shifted towards DNA collection&emdash;British police are now pushing for the DNA collection of children who "exhibit behavior indicating they may become criminals in later life" (Townsend and Asthana 2008), while former New York City mayor Rudy Giuliani has encouraged the collection of DNA data of newborns (Lambert 1998).

When data is collected, whether such data remains used for its stated purpose after its collection has been called into question, even by government officials: the European Data Protection Supervisor has acknowledged that even when two databases of information are created for specific, distinct purposes, in a phenomenon known as 'function creep' they could be combined with one another to form a third with a purpose for which the first two were not built (eGov Monitor Weekly 2006). This non-uniqueness and immutability of information provides great potential for abuse by individuals and institutions.

When is surveillance appropriate?

Many different groups define appropriate bounds for surveillance in different manners. One viewpoint that we have found interesting is that of M.I.T. professor Gary Marx, who argued that before implementing surveillance we should evaluate the proposed methods by asking a number of questions, which we enumerate below:

A. The Means

Harm: does the technique cause unwarranted physical or psychological harm?

Boundary: does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational or spatial border)?

Trust: does the technique violate assumptions that are made about how personal information will be treated such as no secret recordings?

Personal relationships: is the tactic applied in a personal or impersonal setting?

Invalidity: does the technique produce invalid results?

B. The Data Collection Context

Awareness: are individuals aware that personal information is being collected, who seeks it and why?

Consent: do individuals consent to the data collection?

Golden rule: would those responsbile for the surveillance (both the decision to apply it and its actual application) agree to be its subjects under the conditions in which they apply it to others?

Minimization: does a principle of minimization apply?

Public decision-making: was the decision to use a tactic arrived at through some public discussion and decision making process?

Human review: is there human review of machine generated results?

Right of inspection: are people aware of the findings and how they were created?

Right to challenge and express a grievance: are there procedures for challenging the results, or for entering alternative data or interpretations into the record?

Redress and sanctions: if the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillant behavior?

Adequate data stewardship and protection: can the security of the data be adequately protected?

Equality-inequality regarding availability and application: a) is the means widely available or restricted to only the most wealthy, powerful or technologically sophisticated? b) within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist c) if there are means of resisting the provision of personal information are these equally available, or restricted to the most privileged?

The symbolic meaning of a method: what does the use of a method communicate more generally?

The creation of unwanted precedents: is it likely to create precedents that will lead to its application in undesirable ways?

Negative effects on surveillors and third parties: are there negative effects on those beyond the subject?

C. Uses

Beneficiary: does application of the tactic serve broad community goals, the goals of the object of surveillance or the personal goals of the data collector?

Proportionality: is there an appropriate balance between the importance of the goal and the cost of the means?

Alternative means: are other less costly means available?

Consequences of inaction: where the means are very costly, what are the consequences of taking no surveillance action?

Protections: are adequate steps taken to minimize costs and risk?

Appropriate vs. inappropriate goals: are the goals of the data collection legitimate?

The goodness of fit between the means and the goal: is there a clear link between the information collected and the goal sought?

Information used for original vs. other unrelated purposes: is the personal information used for the reasons offered for its collection and for which consent may have been given and does the data stay with the original collector, or does it migrate elsewhere?

Failure to share secondary gains from the information: is the personal data collected used for profit without permission from, or benefit to, the person who provided it?

Unfair disadvantage: is the information used in such a way as to cause unwarranted harm or disadvantage to its subject?

In general, we feel that surveillance can be ethical, but that there have to exist reasonable, publicly accessible records and accountability for those approving and performing the surveillance in question.