

Smile, You're on Candid Camera: Changing Notions of Surveillance in Postmodern American Culture

Kevin Mahaffey

Director of Software Development, Flexilis

Abstract:

Recently, surveillance has become somewhat of a pop-culture fascination. From the Reality TV shows permeating every network's line up to the webcam phenomenon of the late 1990s, surveillance has become more a source of entertainment than ever before. Benjamin Franklin's quote, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety," has long served to exemplify the American, "Big Brother," notion of surveillance: that the government is the main aggressor and seeks to take away privacy and thereby, liberty. My talk will contrast traditional perceptions of surveillance in American culture with new notions brought forth in the emerging digital economy. The privacy of individuals is being bought from individuals through tangible or intangible rewards and resold as demographic data to the highest bidder. Instead of resisting the reduction of privacy, people are embracing surveillance as a benign improvement of everyday life. If we continue such a trend, will society be better for it, or will ubiquitous surveillance serve to implement Orwell's nightmare in *1984*?

Presentation Outline:

You already have zero privacy. Get over it.

—Scott McNealy,

CEO Sun Microsystems, 1999

- 1) Privacy issues are overwhelmingly centered on government interaction with individuals.
 - a) Such is the *disciplinary* notion of surveillance: technology is used to enforce laws and punish offenders. There is no direct benefit for the individual.
 - b) Thereby, a culture of mistrust for government surveillance powers has formed, reinforced by everyday examples of the evils of government surveillance:
 - i) Dystopian literature: 1984: big brother and telescreens
 - ii) *Real totalitarianism*: Nazis, Bolsheviks: concrete examples of the faults of disciplinary surveillance
- 2) Parallel to the growth of government surveillance Commercial surveillance has taken root.
 - a) Began in the 19th century to combat anonymity and the risks of not knowing the financial and moral past of the person with whom you are dealing.
 - i) The unidentified American—we find him everywhere where trouble is. (New York Times, 1912)
 - b) Two Brothers by the name of Tappan started interviewing and keeping records on all of the merchants they dealt with.

- i) Not long after this practice began, the whole business community saw the value of commercial records on individuals and the brothers opened the first privately owned credit reporting agency.
 - ii) Soon, this agency had over 10 thousand agents, including Ulysses S Grant and Abraham Lincoln
 - iii) The agents reported on everything from the worth of your home or farm to the drinking habits of your wife.
 - iv) This system created very detailed reports of many Americans, but was not authoritative in identifying anyone.
- 3) The leap toward authoritative identification in commercial surveillance interestingly had roots in the government
- a) Roosevelt's Social Security Proposal included a unique number that would positively identify every U.S. citizen; however, he promised that it would only be used to dole out benefits. Never would it be shared with law enforcement. Thus, the public accepted social security numbers as a form of identification strictly for government purposes until the mid 20th century.
 - b) As consumer reliance on financial services grew, so did fraudulent uses of those services: financial institutions turned to SSNs as a source of universal authoritative identification
 - i) The public had practically no choice in the matter because the benefits provided by the financial institutions far outweighed the seemingly small loss of privacy entailed by handing out a 9 digit number. If someone refused to give his or her number, they could not have their paycheck honored, they could not get any credit, and they could not get any form of insurance.
 - c) This step, the commercial use of the social security number, made possible, for the first time in history, the link between financial, health, and public data in privately owned databases.
- 4) Since then, Commercial surveillance has overtaken government surveillance.
- a) Commercial surveillance, from its inception, has not been seen as a threat as has government surveillance...
 - i) ...mainly because it is in the background, non-invasive, and never used for punishment, but rather to determine some sort of benefit for the consumer (loans, check

- b) One congressman has admitted “Big Brother has simply subcontracted out to Corporate America.”
- 5) Today: the commercial surveillance that was previously to identify risk in financial transactions is now primarily used by advertisers and marketers to create *demographic categories* of individuals.
 - a) The passive monitoring of previous commercial surveillance is not enough
 - b) Reality, the previously discarded, mundane details of daily life matters more than ever.
 - c) *The details of everyday life require invasive and constant surveillance normally associated with government surveillance*
- 6) The focus of my research is the public’s embracing surveillance as normal when employed by commercial interests, thereby becoming nonchalant in their reaction to increasingly invasive surveillance mechanisms.**
 - a) The bottom line is that companies give incentives or rewards so that people willingly submit to increasingly pervasive surveillance
 - b) The Pop Culture obsession with surveillance evident in the webcam and blogging movements also promotes a positive attitude toward commercial surveillance.
 - c) With acceptance to surveillance comes habituation: younger generations are born with it, see it is normal, and will naturally accept it: surveillance is self perpetuating
- 7) Interestingly: Reality TV exemplifies the incestual circles of the “privacy market”
 - a) Example: one show, Big Brother
 - i) Housemates for a chance at fame, celebrity: sell their privacy
 - ii) Likewise: for the promise of interactivity in chat rooms and forums: consumers go onto the show’s web site
 - (1) In order to access certain portions of the site, they have to provide demographic information, and often elect to participate in surveys
 - (2) >From the provided information the producers can use data mining software to alter the way the show is presented to optimize ratings.
- 8) More detailed forms of data mining will emerge as we find more interactive ways to deliver content.

- a) Using data mining to deliver demographic content has already taken hold in internet media in ad networks such as Google's AdSense which displays ads based on the content of the page, the user's previous click through habits, and the user's geographic location.
 - b) One scholar presents the newspaper as an example of the benefits of demographic data mining for both consumers and content producers
 - i) Marketers nightmare: 100 pages
 - ii) Men passing over women's clothing ads, children passing over shampoo coupons
 - iii) Demographic data
 - (1) Content, ads you want
 - c) Free-PC.com was created at the height of the dot-com era and would give any person a free computer and internet access in order to monitor their browsing habits and display ads on the screen at all times.
 - i) The blatant breach of privacy succumbed to the almighty power of free and the company received 300,000 applications on its first day of operation.
- 9) As convenient as consumer ranking and categorization would seem to be, there are inherent practical problems not usually addressed by objectionist groups that condemn commercial surveillance based on the simplistic notion that privacy is good therefore surveillance is bad:
- a) Database categorization creates a new age of automated discrimination
 - i) Some phone company call centers now have a system in place that ranks each caller automatically as a red, yellow, or green depending on how much profitable they are for the company.
 - ii) Operators are instructed to bend over backwards for greens and cut deals for them whenever they are requested, be polite to yellows, but never discount services, and essentially ignore reds and not waste company time on them.
 - b) How do you fix your ranking? You cant just get out of the system and refuse to participate or your ranking will not improve and you gain no ground
 - i) Counter-intuitively, you have to go further in and generate more data
 - ii) This is the vicious cycle of commercial surveillance

iii) Tivo is a great example of this predicament. It reports every show you watch to the main headquarters, classifying viewers by their tv decisions.

(1) There was one straight Los Angeles man classified as gay, and thereby the tivo recorded a lot of gay programming

(2) To combat this, the man sat in front of the tv for hours watching War movies and other “guy stuff”

(a) Tivo’s database mining software extracted a fixation with violence from these new viewing habits and began recording documentaries on Joseph Goebbels, classifying the man as a neo nazi

10) Eventually the pop culture fixation will disappear, and we will be left with surveillance infrastructure and a habituated public

a) Then, it will be nearly impossible to get rid of the new wave of privacy elimination.

b) We need human accountability: right now there is only trust accountability. If you don’t trust the company, you refuse to use their services and buy their products.

i) This becomes more complicated, however, when companies employ “spyware” that is not easy (and often impossible) to remove for the average consumer.

c) Once the data is gathered, it is seemingly harmless when in commercial hands because it will likely only be used to display targeted advertisements; however, what if governments buy databases or simply seize them from these companies?

i) In the 80s, kids gave their birthdates and addresses to one ice cream parlor in order to get a free ice cream cone on their birthday.

ii) The U.S. government proceeded to buy this database database, and mailed out draft registration cards on the kids’ 18th birthdays.

iii) The evolution of surveillance is such that the incentives given to consumers to get them to surrender their personal data are worth far less than the data itself.

Sources consulted:

Andrejevic, Mark. *Reality TV: The Work of Being Watched*. Lanham, MD: Rowman & Littlefield Publishers, 2004.

Armstrong, Gary and Norris, Clive. *The Maximum Surveillance Society: the Rise of CCTV*. Oxford: Berg, 1999.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, MA: Addison-Wesley, 1998.

Foucault, Michel. *Discipline and Punish*. New York: Vintage Books.

Orwell, George. *1984*.

Palmer, Gareth. *Discipline and Liberty: Television and Governance*. Manchester, UK: Manchester University Press, 2003.

Parenti, Christian. *The Soft Cage: Surveillance in America from Slavery to the War on Terror*. New York: Basic Books, 2003.

Staples, William G. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowman & Littlefield Publishers.

Zaslow, Jeffrey. "If TiVo Thinks You Are Gay, Here's How To Set It Straight --- Amazon.com Knows You, Too, Based on What You Buy; Why All the Cartoons?" *The Wall Street Journal (Eastern Edition)* Nov. 26 2002: A1.