THE EVOLUTION OF SURVEILLANCE TECHNOLOGY BEYOND THE PANOPTICON

by

Michael Luke Bullock

A Thesis Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Fine Arts

in Digital Art and New Media

at

The University of California Santa Cruz

March 2009

Thesis Committee:

Catherine M. Soussloff, Ph.D. (Chair)

Peter Elsea

Dard Neuman

Abstract

The subject of the evolution of surveillance and its incorporated technologies is a topic that is important to examining the state of surveillance and its impacts on contemporary society. Likewise this subject is also an important informant to my work as an artist in the field of new media as it seeks to examine the art and technology of surveillance and its existence in today's society as a system that we are able to employ for our own benefits and security. This paper attempts to summarize the tumultuous history of the technologies associated with surveillance from Colonial America to the present and through this summary examine the shift from post facto disciplinary practice to a real-time practice revolving around the security and conveniences it offers participants.

Foucault and the Shameful Art of Surveillance

Foucault saw surveillance as a "shameful act" of supervising and imposing discipline on a subject through a hierarchized system of policing.[1] He analyzed the systems of social power through the lens of the 18th century philosopher Jeremy Bentham, the originator of the now iconic Panopticon. This Panopticon was, and is, a design for a prison in which the inmate's cells are arranged in a circular fashion around a central guard tower. The architectural configuration allows for a single guard's gaze to view all inmates, but prevents those inmates from knowing exactly when they are being watched. "The major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power."[2] Foucault viewed this design as a "generalized model of functioning and a way of defining power relations in terms of the everyday lives of men."[3]

He also saw surveillance as a decisive economic operator as an internal part of the production machinery and as a specific mechanism of disciplinary power. In this model of power surveillance acts as a mechanism of control by those with authoritative status in political and economic spheres, a way of disciplining the subject into a productive member of society. Foucault also manages to connect the invisible authority of the Panopticon to the very visible authority given to the syndic during the era of the plague. The syndic, specifically, was an agent of discipline, which assured that a town's inhabitants were safely locked away from those bearing the illness of the plague and consequently each other. The syndic was responsible for monitoring and emptying his prescribed streets of people on a nightly basis. Though a form of authority himself, the syndic was not free of his authoritative figure as well, for if he should abandon his street

he would be condemned to death himself. In each of these examples the subject is seen but does not see; he is the object of information, but never a subject in communication.[4]

One must understand that this paper does not attempt to vilify the valid historical observations and analyses of Foucault's writings and lectures on the structures of power, analyses that have defined how we view the beginnings of control and discipline in modernity, but attempts to offer an alternative view to many contemporary critiques of surveillance society that embrace this basic model and forego the copious changes in technology that have remodeled society and surveillance. The Foucauldian model of analyzing surveillance and its power structures may have held true in the 18th century and even up to the time of Foucault himself, but revolutions in technology have since marked it as outdated. In order to understand how Foucault's Panoptic model no longer applies to current surveillance practices and technology we must understand the changes that have occurred in surveillance technology since its beginnings. Changes that have migrated surveillance from a practice of post facto action with the ultimate goal of disciplining, or imposing self discipline upon the subject, to a real time practice of informing, securing, tracking, and communicating with its subjects.

The Origins of Surveillance in Colonial America

The origins of surveillance in the United States emerged during the turbulent years of slave trading in the nation's colonial history. These early examples of surveillance systems developed mainly in the southern states and manifested in the forms of published appeals, and memorandum books.[5] Each of these bits of technology

revolved around the movements and activities of commodities both agricultural and human. Many slave owners carried with them small ledgers in which they wrote reminders, reading notes, accounts, descriptions of plantings, inventoried their crops and livestock. These memorandum books would also include notes on slave movements and activities around the plantation.

Occasionally crops, or livestock, even slaves would go missing. Missing crops and livestock can be troublesome to track down, and people even more so. When slave owners were tasked with tracking down a runaway, many would publish an appeal for the capture and return of the offending commodity. Published appeals surfaced this way as a form of published news paper article detailing the physical and characteristic traits of "truant" slaves and servants, many offering rewards for the return of said slaves. In his book *Soft Cage* Parenti reprints an ad originally from the November 21, 1745 *Virginia Gazette* that reports a detailed description of a run away slave along with a note that he could have a "great Acquaintance" that provided him with a false pass This notation of the possibility of a 'false pass' brings us to the subversion of one of the three key surveillance technologies of the colonial era, the written slave pass, organized slave patrols, and wanted posters detailing runaway slaves.[6]

Not all slaves caught off the plantation were runaway slaves, many possessed a pass to move about at their master's will. This pass, an embryonic form of the modern ID as Parenti puts it, first surfaced in 1642 Virginia law and targeted poor white indentured Irish servants attempting to flee their work obligations. Any white person leaving the colony required a pass from the colonial governor to ensure that they were not fugitives or debtors. By 1656 even Native Americans entering the colonies to trade had to carry

"tickets" issued by the colonial authorities. The laws surrounding these passes though made no mention of slaves until an exclusive slave pass law was enacted in 1680 Virginia.[7] South Carolina followed suit in 1687 with lawmakers setting forth a decree that "it shall not be lawful for any negroe or negroes, or other slave, upon pretence whatsoever to travel or goe abroad from his or her master or mistresses house in the night time, between sunsetting and the sunrising, or in the day time without a note from his or her master or mistresse or overseer."[8] These rudimentary ID's often made no attempt to describe the physical characteristics of the slave. Many were as simple as primary school hall-passes, consisting of merely the name and destination of the slave and signed by their owner. The passes relied mainly on the assumptions that slaves were illiterate and the patroller's personal knowledge of the master's name.

Patrollers were often middle class property-owning civilians and whose chief functions were surveillance and corporal punishment. Patrollers often rode under the cover of night in "beat companies" of three to six men armed and empowered to search homes for runaways, weapons, or supply caches that might indicate plans of escape. Black people negotiating the roads at night would be required to produce either written passes from their masters or "freed papers," proof of their emancipation, otherwise they would face the whip or worse. Some regions paid their patrollers with tax money, effectively creating a tributary to the modern police, but more often their work was a form of taxation , or corvee labor, levied upon all white men. In either case patrollers were frequently offered, or demanded, bounties from the owners of runaway slaves.[9] Though patrollers were often residents in areas where populations were low, it was still unlikely that every patroller knew every slave by sight and as such the forgery of slave

passes and manumission documents became a serious problem. In 1783 South Carolina authorities adopted a new technology for monitoring slaves.

This new mode of identification was the brass or tin slave "tag" required by urban slaves that wished to hire themselves out for their masters as wage laborers. This badge was stamped with the slave's occupation, the date, and a number to record payment of the slave tax each year. Similar badges existed for free Blacks as well; each prefabricated, metal, and cross referenced to city records, artifacts far more difficult to forge than written passes and "freed" papers. These badges served both as a form of collecting revenue and also as a system of political control of African American people as a class. Parenti includes an account of this effect by the fugitive John Andrew Jackson. The excerpt details how Jackson was influenced into hiding after joining a work gang and finding out that any negro found working aboard their vessel without a badge was liable to be put in jail.[10]

Even with these systems in place resistance was still empowering slaves with forged passes, fake papers, and new identities. In response to the success of slave resistance and escape, planters made more *post facto* attempts to identify their truant captives with elaborate wanted posters and ads using increasingly standardized descriptions for identification.[11] These descriptions constituted a sort of biometric identification after the individual had already gone missing, including height, complexion, demeanor, intelligence, age, sometimes even describing the teeth of the slave. The wanted posters and ads were exemplary of both antebellum social control and of the technical inadequacy of that system; biometric identification was applied only after the fact.

The next practical leap in identification came during the Civil War with military passes issued for anyone moving about the nation. These military passes were common to both the Union and Confederacy. Both armies had similar criteria listed on their passes including name, age, height, eye color, hair color, along with more subjective descriptions such as peculiarities and shapes of mouths, noses, and chins. The origins of passes such as these date back to ancient times and documents of safe passage, a form of primitive passport. As early as the 1820s official US passports contained elaborate descriptions of the bearer. Though these physical details were often listed in vague terms such as Passport No. 992, issued to John Finney in 1826 that lists forehead, nose, and mouth as "common" with a "roundish" chin.[12]These passports and military passes are some of the contributing origins to modern technologies of identification and registration. As so, these technologies would be repurposed after the end of the Civil War, slavery, and the radical reconstruction into the realm of criminal justice and the control of immigrant labor.[13] At the same time new technologies such as the advent of photograph and precisely recorded body measurements, became available, allowing a deepening of everyday surveillance and discipline.

As a response to rising and prolonged organized violence many cities followed the lead of London's 1829 creation of the first modern constabulary.[14] In 1836 officials in New Orleans created the first full-time civilian patrol with Philadelphia and Boston starting similar programs around the same time. It was New York though that established the first full-time armed police force in 1845. The primary task of these police forces was, like it is today, "maintaining order. " This was generally accomplished by controlling petty offenses, but with mass immigration and industrial urbanization these

forces were confronted with the need to discover and tag new criminals, not simply those "known to the community." This advent of professional police forces also coincided with the proliferation of photography and police use of this new technology to identify and tag prisoners and criminals.

In 1839 Louis Jacques Mande Daguerre and amateur scientist Joseph Nicephore Niepce came together and produced permanent photographic images requiring only twenty-minute exposures. These glass-plate daguerreotypes gained great mass appeal within the following years and as they did the technology improved and exposure time dropped. In 1841 cheap, quick paper prints became available, competition increased, and prices fell even further. The realism and price of this new information technology made it perfect for adoption by the newly formed police departments.

1853 saw the New York Police Department beginning to catalogue photographs of repeat offenders and publishing their images in a "rogues' gallery."[15] Philadelphia, Albany, and a handful of other cities opened similar galleries as well; in all cases the public was "invited to call and examine." By 1858 the NYPD had 450 "abrosetypes," a type of glass plate photograph, displaying habitual offenders, and a few years later most major departments from Moscow to San Francisco had also opened rogues' galleries.[16]

The problems with rogues' galleries surfaced as more and more police photographs were produced. The more images police produced, the harder it became to sort, organize, and effectively use them. With thousands of images on file, how were the photos to be archived? By 1912 the mug shots in the NYPD's rogues' gallery were posted on broad, yardwide panels, each of which was mounted on hingers and allowed to

turn like wall mounted books. Each two-foot by three-foot page had ten rows of twelve wallet size photos; hardly a convenient way to pinpoint a single person. Even juries in the UK found that the sheer size of the list of names and catalog of photographs caused them to be useless as a means of identification.[17] What police needed were reliable methods of indexing their photographs. While US police forces were struggling with these photos the Scotland Yard was adopting a new system after the passage of the Habitual Criminals Act.

Britain's Habitual Criminals Act of 1869 required police to keep an "Alphabetical Registry" and cross-referenced "Distinctive Marks Registry. The first held names, and the latter descriptions of scars, tattoos, birthmarks, balding, pockmarks, and other distinguishing features. This registry of marks was systematically disaggregated into nine general categories pertaining to regions of the body. Therefore there were files for the head and face; throat and neck; chest; belly and groin; back and loins; arms; hands and fingers; thighs and legs; feet and ankles. Police were tasked with checking first the Alphabetic Registry for an arrestee's name hoping to find a corresponding photo and file. If that failed the clerk would then search the prisoner's body for any distinctive marks and then check one of the nine body-area files for a match. Though still an irksome way to track down a singular person, it was far better than searching through thousands of photographs on display. This system, like the wanted posters, ads, and passports of the slave and Civil War years, attempted to collect the information surrounding the body of the individual. Unlike the previous attempts though, this registry of names and distinctive marks begins to herald a new mode of logging and accumulating of data pertaining to people. This shift was away from trying to identify the individual by sight alone and

instead looked to the information of the body, or biometrics for tracking the misdeeds of the criminal.[18]

By the late 1870's a new system of cataloguing and retrieving police files dubbed "Bertillonage" had come into practice in European prefectures. This system, pioneered by Alphonase Bertillon, a clerk with the Parisian police was adapted from his father's and brothers' anthropological practice used to discover "racial phenotypes" through the measuring of "savage" bodies.[19] Bertillon's regimen of body measurement identification soon became even more trusted than the photography it was supposed to index. In his system each prisoner's dossier held a card containing the usual mug shot and description of distinguishing marks, as well as eleven different categories of exact bodily measurement. Each numerical value was the product of a highly choreographed scientific procedure in which only a trained "Bertillon operators" would manipulate and measure the prisoner's body from head to toe. The operator's aim was to garner from the body a set of constant, nonsubjective measurements that could be recreated exactly by any other operator using calipers in exactly the same way. These sets of data were translated into an elaborately coded vocabulary that allowed the numerical data to be easily telegraphed or shared with departments in other jurisdictions. The repeat offender could no longer hide behind an alias, disguise, or even years of aging. Bertillonage was not perfect though; the practice still had its weaknesses. Capturing exact measurements required extreme precision and consistent procedures. To achieve this precision Bertillon created a Taylorized choreography of movements that the operators were required to follow in every minute detail. The foot alone required twenty exact movements or proper measurement. The problem was every operator did not utilize the same movements or

codes, and many police forces simplified the process as they saw fit. These versions of the system were so altered that soon they only worked in relation to themselves and as soon as the prisoner's data was traded across jurisdiction it became useless numerical noise. Though a valuable system, the overly complex nature of Bertillonage was waiting to be replaced by better.[20]

During the late 1850's the eccentric Francis Galton, father of eugenics and cousin to Charles Darwin, conducted experiments that yielded a system of classification that looked at the papillary ridges of the fingertips.[21] This system divided all human prints into three subpatterns: loops, whorls, and arches. These categories were refined and broken into even smaller subsets by a colonial administrator named Edward Henry. However the idea of using dactyloscopy, or fingerprinting, for criminal identification did not surface until 1880 in a letter to the publication *Nature*, from a British physician by the name of Henry Faulds.[22] Historical records offer conflicting accounts as to which constabulary force first deployed dactyloscopy, but by 1902 the practice had moved from colonial territories in India to the heart of Scotland Yard, migrating from colonial periphery to economic core. The first real working fingerprint file in the US was created by police administrators for monitoring would be police applicants to combat cheating on entrance exams.[23] However the fingerprinting revolution in the US was not sparked until John Kenneth Ferris, a young Scotland Yard detective, gave a stirring demonstration of dactyloscpy at the 1904 St. Louis World Fair. Within a few years of the fair major police departments in Boston, Baltimore, Washington D.C., St. Louis, Cincinnati, Cleveland, Louisville, Indianapolis, and Memphis had all adopted the practice of fingerprinting their criminals. In 1907 the Navy also adopted dactyloscopy in an effort to bust deserters. It

was two years after the fair when the NYPD applied the technology to its Bertillon files. Leavenworth Penitentiary followed suit and these files formed the basis of the federal government's first National Identification Bureau, the predecessor to the FBI's Bureau of Identification.[24] The system finally paid off in 1910 when prosecutors and cops had their first criminal convictions based on fingerprints. The defendant in this landmark case was an African American man accused of robbing and killing a white woman. The only evidence against housepainter Thomas Jennings was a set of prints left in the tacky paint on a piece of porch railing. Police removed the piece of railing and found the prints to have thirty-three points of similarity to Jennings'. The case went all the way to the Supreme Court, where Jennings' sentence of death was upheld, and with it the place of dactyloscopy in identification, criminal and otherwise, was solidified.

A Brief History of Audio and Visual Electronic Surveillance

David Morton's online resource for the history of recording technology supplies us with a history of the use of electronic communication technology in the surveillance society.[25] He begins by discussing the origins of wiretapping citing the earliest known use of electronic surveillance in the US. The earliest known case of electronic eavesdropping took place under the administration of President Lincoln when both sides involved in the Civil War would tap into each other's telegraph lines and simply copy the messages being communicated. The advent of the telephone made wiretapping somewhat more difficult, as the rate of information flow on the telephone was much faster. For many years, there was no easy way to record telephone calls and law enforcement officials who

wanted to listen in had to transcribe conversations by hand. The desire for a telephone recorder for legitimate business purposes was one of the inspirations for Thomas Edison's phonograph. Yet the phonograph was not yet sensitive enough to do the job.

The telegraphone, the first magnetic recorder, was specifically designed to record directly from the telephone lines. It was also described by its inventors mainly as an office dictation machine or crude voicemail system. However, the American Telegraphone Company, which made the telegraphone under license in the U.S., and its distributor on the West Coast introduced the idea that sound recording could also be used for surveillance. A 1906 article, probably written by an American Telegraphone official, describes a scene in which a fictitious Mr. Brown and Mr. Jones argue over what was said during a conversation, ultimately ending with Mr. Jones replaying a recording of the words in question. Unfortunately, the American Telegraphone Company failed without producing very many machines, so there was little chance for its use to become common.

About the time of World War I, the Dictaphone Corporation introduced a new, phonograph-based recorder capable of recording from the telephone lines. AT&T forbid its use on the public lines, although a few were used by power companies and railroads on their private lines. Recording devices were rarely used for surveillance in the United States in the period from the introduction of the telegraphone to the end of World War II, despite the many suggestions that they would be useful for this purpose. Instead, improved electronic devices like the Dictagraph (not made by Dictaphone despite the name) were popular among private detectives and the police.

A major shift came after 1945, when wire and tape recorders became available. While they were not usually advertised as such, many users modified them to make surveillance recordings. The first discussions in the courts of whether or not sound recordings could be admitted as evidence began to appear at this time. The making of secret recordings began to be a common element in the plots of novels and movies, but the size of the machines and their general lack of portability probably made their actual use much less common than that. It was not until the introduction of the transistor recorder in the early 1950s that secret recording became more common. Shortly after "pocket" size tape and wire recorders appeared, certain companies began promoting their use to make secret recorders. The Minifon, a West German product, was the best known of these. As Cold War paranoia grew, so too did the making of these secret recordings.

The best-documented cases of individuals (rather than law enforcement officers, intelligence operatives, or private detectives) using surveillance recorders extensively come from the offices of U.S. Presidents. Although Franklin Roosevelt briefly used a special telephone recorder in the 1940s, after World War II the general availability of these machines helped them find their way into the Oval Office. Truman used a wire recorder; Kennedy a dictation machine. The scandal that erupted over the infamous "Watergate Tapes," however, brought the matter to the public's attention. Nixon was an avid user of office dictation machines, but he also made recordings of telephone and office conversations without knowledge of the participants. He considered them a form of record keeping.

Today the use of audio surveillance is arguably a minor issue compared to the massive use of video and Internet surveillance. What is being done with technology today

is not different in principle that what was done a century ago, but today it is undeniably more sophisticated. Following closely on the heels of the technological advancements of audio recording was the technology of visibility and image recording.

After the invention of photography brought about the revolution of motion pictures it wasn't until 1927 that Philo Farnsworth was able to devise a way of transmitting images from a camera to the cathode ray tube television systems. The next important step in video came in 1951 when Charles P. Ginsburg developed the first practical video tape recorder. The recorder captured live images from television cameras by converting the information into electrical impulses and storing them on magnetic tape. This method had been explored before, magnetic tape had previously been used in audio recording, but the main problem was that the bandwidth, or data capacity, of magnetic tape media for recording audio was insufficient for the amount of data produced by electronically capturing sequential images.

If you consider video in the simplest of terms, video surveillance began with simple closed circuit television monitoring. As early as 1965, there were press reports in the United States suggesting police use of surveillance cameras in public places. In 1969, police cameras were installed in the New York City Municipal Building near City Hall. The practice soon spread to other cities, with closed circuit television (CCTV) systems watched by officers at all times.

When videocassette recorders hit the market, video surveillance really hit its stride. Analog technology using taped videocassette recordings meant surveillance could be preserved on tape as evidence. The seventies saw an explosion around the world in the

use of video surveillance in everything from law enforcement to traffic control and divorce proceedings. England installed video surveillance systems in four major Underground Train Stations in 1975 and began monitoring traffic flow on major highway arteries about the same time. In the United States, the use of video surveillance wasn't quite as prevalent until the 1980's for public areas, but storeowners and banks quickly understood the value of it.

> *"Retail customers are increasingly comfortable with CCTV surveillance. A security industry official contends that, 'years ago shoppers objected to electronic eyes recording their moves; today it's not only accepted, it's preferred.' "*[26]

The insurance industry also found video surveillance compelling in worker's compensation fraud, bogus accident claims and a variety of other cases began to turn in the industry's favor when they could provide tapes of supposedly disabled workers doing the limbo at a family reunion. However for the private citizen, analog technology was primarily used in the 1970's and 1980's for capturing the worst side of human nature, cheating spouses and poor parenting. Private detectives were able to provide more graphic and compelling evidence of affairs and parental stupidity with film than with still shots, and videotapes became frequent evidence in family court.

The next step was the Charged Coupled Device camera (CCD), which used microchip computer technology. These new cameras broadened the practical applications of video surveillance by allowing low light and night recording possible.

In the 1990's digital multiplexing made great strides in the advancement of practicality in video surveillance. When digital multiplexer units became affordable it revolutionized the surveillance industry by enabling recording on several cameras at once (more than a dozen at time in most cases). Digital multiplex also added features like time-lapse and motion-only recording, which saved a great deal of wasted videotape.

By the mid-1990's, ATM's across the United States and in most parts of the world had video cameras installed to record all transactions. After the first attack on the World Trade Center in February of 1993, the New York Police Department, FBI and CIA all installed surveillance cameras throughout the area. Soon many countries were also using either CCTV or video taped surveillance to cover major sporting events that could be potential hot spots, including the World Cup Soccer games at Giants Stadium in 1994.

The images recorded digitally were so much clearer than the often grainy images recorded with analog that recognition was immediately improved for police, private investigators and others utilizing video surveillance for identification purposes. With digital technology you could also manipulate the images to improve clarity even further by adding light, enhancing the image, zooming in on frames, etc.

The first U.S. city to implement a citywide closed-circuit television surveillance system was Washington D.C. In 2002 the District's police began constructing a centrally monitored, citywide CCTV system which the Metropolitan Police Department (MPD) plans to outfit with 700 cameras, watching streets, schools, Metro stations, federal buildings, and even parts of a Georgetown business improvement district. All images are streamed directly to the MPD's "NASA-style" Joint Operations Command Center filled

with video recorders, computers, and communications gear, and is staffed by the D.C. police, Secret Service, FBI, among other agencies.[27]

These cameras are already spreading across the United States. The RAND Law Enforcement Technology Survey found that 41 percent of local departments and 66 percent of state police departments used "fixed-site video surveillance cameras." In Oakland, California, over seventy surveillance cameras watch the civic center and a duplicate system exists around the Yerba Buena Center for the Arts in San Francisco.

Santa Rosa, California also has cameras watching its Courthouse Square and "Transit Mall." Baltimore has video cameras scanning 106 of its downtown intersections. Tampa, Florida, has even installed thirty-six digital cameras equipped with biometric face recognition software. From coast to coast "cameras continue to sprout up so fast it's impossible to monitor their proliferation adequately."[28]

> *"In reality, the emerging architecture of the soft cage of total surveillance is perhaps the most frightening because it is so mundane, decentralized, and even convenient."*[29]

The Computerization of Personal Information

Instead of the watchtowers, checkpoints, and black helicopters of dystopian fantasy, innocuous passwords, swipe cards, automatic toll lanes and workplace IDs characterize our emerging surveillance society. The landscape is now dotted with registration kiosks -ATMs, automatic ticketing machines, electronic tolls- where we

deposit our personal information in exchange for goods and services. We are not "being watched" so much as we are "voluntarily" checking in with authorities.[30] Today we carry credit cards and bank cards that informally log our movements and lifestyles more effectively than any past efforts. When viewed separately each component of the new digital surveillance seems quite reasonable, but each new camera, database, or ID works in concert to a larger systemic momentum towards increased observation. As technology spreads, surveillance becomes more automatic, anonymous, decentralized, and ubiquitous.[31]

At the core of these technologies lies the modern equivalent of the "Pascaline," the first calculating machine. Built by Blaise Pascal in 1645, the Pascaline used a series of gears to complete calculations.[32] By 1694 Gottfried Wilhelm Leibniz had stepped up the technology by adding a stepped cylinder to Pascal's design. This gave the machine the ability to dived and extract square roots without error. The next real breakthrough came 150 years later when Charles Babbage invented the "Difference Engine," a contraption able to automatically calculate logarithms. Babbage would follow the Difference Engine with the never produced designs for the "Analytical Engine." This second "engine" is now recognized as the basic template for modern computing.[33]

Although Babbage may be heralded as the harbinger of modern computing its real birth was brought about by a young clerk with the US Census Bureau by the name of Herman Hollerith. As a clerk with the Census Bureau Hollerith spent the early 1880s devising an automated means to tabulate the nation's decennial count. At that time the census was tabulated almost entirely by hand and took nearly a decade to complete.[34] By 1884 Hollerith had a patent and a solid prototype of his new tabulating machine. The

machine worked by automatically detecting and counting holes that were punched in census cards. The machine could also aggregate and disaggregate the cards according to different combinations of variables. The census used a card set with standardized holes, each representing a different demographic trait - national origin, gender, age, occupation. By 1890 Hollerith's new Tabulating Machine Company was under contract with the Census Bureau to analyze the year's count. Thus began a true revolution in political record keeping and informatics in general.

Identifying Americans for taxation and credit

In 1935 Franklin Roosevelt's administration passed the Social Security Act beginning the issuance of the Social Security Number and the registration of the American Populace into a massive database. By 1945 the SSA's eight-column punch card's formed a database that took up an entire six acres of storage. Eleven years later the administration had switched from punch cards to an IBM 705 vacuum-tube electronic computer.[35] By the 1960's the SSN was adapted by the Internal Revenue Service as an individual taxpayer identification number. In effect this permanently linked financial and personal data such as residence, employment, and medical history to the social security number. This illuminated huge fields of demographic data and began the demolition of one of the most important firewalls in the structure of modern privacy.[36] Meanwhile more and more business expanded the Social Security number's function creep by demanding it as mandatory ID in ever more contexts.[37] This use of the SSN as a "unique personal identifier" was to everyday surveillance as the discovery of longitude was to navigation.

Now disparate informational snippets like bank records, employment records, health and even criminal records could be accurately mapped and linked to form a coherent picture. With ever-faster computers, increasingly connected through telephone lines, the real distance between these nominally disparate dossiers has been diminishing at an accelerating rate for over thirty years.

In this same period we have also been moving just as steadily to an economic system based in cashless digital transactions. This slow migration toward electronic money, while increasingly convenient, is in some ways the most frightening threat to privacy yet. Electronic money in the broadest sense is almost always linked to one's identity and creates a traceable record of time, place, and exact contents of each purchase. In a society where everything has a price tag, the evolution of a cashless economy is also to be understood as the rising spectre of the panopticon: life under threat of total observation. Leading us along this path of diminishing privacy into a future forged with the merging money and identity is one of the staples of modern economic life, credit cards.[38]

The records produced by credit cards, bankcards, discount cards, Internet accounts, online shopping, travel receipts, and health insurance all map our lives by creating digital files in massive corporate databases. The more we shop with credit or prepaid point-of-sale cards, the more we feed the fragmented but ubiquitous commercial surveillance machine.[39] Like the computers facilitating the commercial surveillance machine, the modern credit business and its aggregation of the populace has its origins in the 1800s. During the 1800s Arthur and Lewis Tappan were New York merchants who supplied goods to the booming towns and farms of the hinterland and frontier. The

Tappan brothers extended credit to over the sprawling geography of the expanding nation. These brothers kept detailed ledgers as risk analysis files describing the individuals interviewed by Lewis prior to the extension of a line of credit. Further interest came with the brutal depression of 1837. Businessmen who survived the depression emerged more wary of risk and with considerably less capital than before. Soon the demand for the Tappan's information soared, and by 1841 the brothers had turned their private dossiers into the first national credit reporting service, which the called The Mercantile Agency. By the early 1850s the Mercantile Agency had branch offices in Boston, Philadelphia, Baltimore, Cincinnati, and New Orleans, and its dossiers contained thousands of pages, updated by thousands of "reporters" and correspondents. By 1924 the Associated Credit Bureaus reported 267 such agencies nationwide; in twenty-four years that number had swelled to 1,453; ten years later it was 2,038. In 1933 Dun and Bradstreet merged to form one of the largest credit rating and financial reporting services in the world.[40]

The earliest cards that carried these sorts of credit lines had a rather mundane beginning at the counters of large department stores. In 1914 Western Union also began providing metal charge cards to selected customers for "deferred-payment privileges." In the early 1920's General Petroleum Corporation issued similar metal cards enabling employees to buy gas on credit. Later this service was extended to "select customers." Likewise AT&T introduced the "Bell System Credit Card" in the 1930s. Though useful these sorts of forays into a more standardized form of retail credit ended with the outbreak of World War II and the creation of "Regulation W," which was designed to rein in borrowing and spending to route capital toward the war effort. In the peacetime

boom following the war the credit market expanded again. In 1946 during this credit expansion a New York banker developed the Charge-It card, essentially a local-bank issued charge card with limited uses. All of these local experiments eventually came together in 1950 when Frank X. McNamara of the Hamilton Credit Company invented the debt-based payment card for multiple locations. He got the idea from a customer who took out multiple charge cards and rented the cards to his acquaintances. McNamara turned this idea into the now famous Diners Club, a card held by only 200 customers and available for use at twenty-seven Manhattan restaurants.[41]

By the late 1950s a number of banks had begun offering revolving lines of credit that could be paid off little by little instead of all at once. Local banks were increasingly linking up to offer seamless credit card services. Interlink, the largest of such ventures, was launched in 1966 and involved fourteen US banks and created a network for extending retail credit across multiple banking areas. A few years later another combination of banks cropped up as the Western States Bankcard Association introduced the "MasterCharge program" eventually to become MasterCard. Its rival was the huge BankAmericard program that later became Visa.[42]

With the proliferation of plastics, the ready availability of magnetic-strip technology, and the ever better computers the 1970s produced an even more complete and automatic information trail than before. By 1972 the Associated Credit Bureaus of America were building a fully operational network of interconnected databases that would facilitate nearly instant credit and background checks. Amid the financial recession of the 1980s the federal government again accelerated the collapse of privacy.

In 1983 the Office of Management and Budget launched a debt collection system

that for the first time allowed federal agencies to share information on individuals in debt to the government with private credit institutions. In exchange the federal government received direct computer access to the private records of over 100 million Americans. At the same time Visa initiated a computerized dragnet to map and locate business with spending patterns that might indicate fraud or theft. Offending business were cut off and required to use electronic authorization. The flow of ever more detailed and routine information to corporate databases was inevitable. The "consumer" now constructed in the databases of credit agencies as a legal and historically knowable entity was increasingly recruited to self-monitor: corporate omniscience generates consumer accountability. Enmeshed in the matrix of obligation, responsibility, technology, one-way financial transparency, the debtor is rendered accountable and therefore productive and governable. Magnetic-strip-based prepaid debit cards have since been adopted by mass transit systems, telephone companies, pharmacies, and welfare agencies.

Amplifying and extending these practices was the simultaneous growth of digital tags, barcodes and scanners, which give unique identities to inanimate objects ranging from boxes of ice cream to government documents. They were first invented in the 1930s and by 1967 were in regular use when railroads deployed them for tracking and routing freight cars. The black and white stripes hit the retail world in 1973 and by 1983 the national market for scanners and bar codes (Uniform Product Codes) was worth an estimated $325 million per year with a growth of over 30 percent annually. Since then barcodes have found their way onto everything from live turkeys, books, and auto parts to hospital patients and military supplies. Virtually all products now carry a barcode. Credit cards and ATM's document who is shopping, where and when, and the addition of

barcodes makes it possible to tell exactly what is being purchased. If magnetic-strip cards, barcodes, and the like can deposit information, why not create a card that can also gather and sort information? This is the idea behind the "smart card," an ID bearing a constantly updated microchip.[43]

With this "smart card" technology a single card can store and update information on a person's identification, drivers license status, or medical and credit history. The first cards embedded with silicon ships were created in 1974 by a French engineer named Roland Moreno and have since been adopted by several countries as forms of a national ID that stores healthcare information. Visa International, the largest bankcard issuer in the US, in an effort to gauge public response, will allow healthcare providers to store and access a patient's medical history through the new chips in state of the art cards. Such digital miniaturization exponentially concentrates the amount and quality of consumer data available for analysis and resale. Processing or "data mining," the accumulated information from smart-card transactions is the next logical step after their introduction. One specialist who supplies Safeway with high-tech surveillance gear explained upon introducing the store's new ID-tagged discount cards and hidden cameras: "We could monitor how much time an individual spends in the shop and in what order they shopped it. We could learn about any dead-spots in the store as well as what the shopper bought." For example a woman in San Francisco reported that nine months after buying a home pregnancy test from Safeway she began receiving the company's coupons for diapers and baby food, mailed to her home.[44]

Tracing Individual Paths

With advances in Internet technology we see these forms of commercial surveillance racing toward a limitless horizon of possibilities; even now "window shopping" can be recorded, stored, and analyzed in a plethora of ways. One has to recall that credit card numbers and all the information they carry about the owner's age, income, mailing address, and habits are ever present in e-commerce. In addition around over half of all major websites on the Internet employ surreptitiously downloaded programs called cookies that tag, track, and analyze the movements of every user and visitor. Originally developed in 1994 by a programmer at Netscape named Lou Montulli, cookies at first merely identified Internet users when they returned to a website for each visit. Cookies were simply a site-specific form of cyber ID that communicated only with their systems of origin.

Because a cookie is essentially a piece of code that rides silently in the inner workings of one's computer it has the ability not only to monitor what one does on the cookie's site of origin, but also the ability to report back to its home base with details of all the other sites its host computer has visited. Cookies can report on where you've been, how long you've been there, some even have the abilities to count keystrokes, copy whole files, and connect all of this information to the owner's user identification, credit cards, and passwords. To use Foucault's language, cookie surveillance both "individualizes and totalize," creating simultaneously unique individual dossiers and broad demographic profiles.[45]

The firms with the most sophisticated cookies are also the ones that most diligently analyze their data for marketable products. For example the company DoubleClick builds detailed profiles of Internet users and then sends back demographically tailored advertisements. When users visit any of the 11,000 DoubleClick affiliated websites a cookie is placed on their hard drives. Once there it gathers information like usernames, passwords, and preferences, all of which are later uploaded to DoubleClick's central database. The information collected includes names, email addresses, home and business addresses, telephone numbers, searches performed on the Internet, web pages or sites visited and other communications and information that users would normally not expect advertisers to be able to collect. Many individual online stores do something similar such as Amazon.com watching what individual users view and adjusting suggested products accordingly.

The real impact of the Internet on surveillance is still yet unknown, as even today new Internet technologies are emerging that are changing the way we interact with our and each other's information. The Internet not only acts as a vital nervous system for surveillance technologies, conducting data to and from processing centers and databases, it also acts as an emerging surveillance forum where users actively, and voluntarily, participate in their everyday lives. The emergence of social networking sites such as Facebook, MySpace, and Twitter, among a myriad of others, hails the beginning of a new era of "opt in" surveillance where users are encouraged to share their personal activities, information, and thoughts with their peers and even people they have no connection to whatsoever. Not only do these web applications collect personal information in exchange for registration and inclusion, they also provide a canvas that users voluntarily populate

with all sorts of personal information from age, location, education, and relationship status to contact information and personal images. These sort of applications of Internet technology also make it resoundingly easy for employers, relatives, friends, strangers, companies, and agencies to pour through these masses of data willingly offered up by users.

Parenti notes that one can image how law enforcement agencies might wish to cross reference the subscriptions list of Guns & Ammo with online research from police-hating Internet chat sites and available psychiatric medical and insurance records, or the membership lists of "extremist" political organizations.[46] Law enforcement agencies currently wishing to profile any, or all, adult American's can turn to Acxiom Corporation, a giant information service firm operating out of the Ozark foothills. All day, every day, Axciom's computers gather and process information trails left by 196 million Americans. the companies databases haul in information from credit card transactions, magazine subscriptions, telephone bills, real estate records, vehicle registrations, fishing licenses, consumer surveys, and census surveys, to name only a few types of sources. their clients can purchase demographic or individual profiles. According to one report: "Axciom often can determine whether you own a dog or cat, enjoy camping or gourmet cooking, read the Bible or lots of other books. It often can pinpoint your occupations, the car you drive, your favorite vacations." All of this information is based on what users voluntarily supply over the Internet. In the end, all of the fragmented and disparate dossiers of e-commerce and digital bookkeeping are easily united into metafiles, which can be used by both commercial and state agencies.

Credit card agencies are now offering the statistics and information they collect on their customer's spending habits directly to their customers. By doing so they allow them to directly monitor the same purchasing patterns that allow other business to tailor their offers to the same customer's patterns. However credit cards aren't the only way we can be monitored from a distance.

Consider the array of technologies for reading identification codes from a distance. These systems are often referred to as "automatic electronic identification," or when used in conjunction with motor vehicles, "automatic vehicle identification." Some of these systems use mounted or handheld receivers that monitor the energy emitted, or reflected, from a radio frequency identification badge or tag. Other systems use magnetic strips or barcodes that are read when swiped or scanned by properly equipped computers. As with many present technologies, rudimentary systems such as these were introduced in the early 1970s, though as they were unusually expensive the technologies were only used for controlling access to executive suites, military labs, and similar hot spots. By the late 1980s these automatic ID systems were managing inventory, baggage, parcels, and livestock as well as controlling passage in and out of restricted, security-sensitive locations.

Beginning in 1988 a number of regional transportation authorities began using an experimental form of automatic toll payment technology based on automatic vehicle identification. One of the first systems to go online was the North Dallas Tollway, using electronic identification technology developed in the early 1970's for high-security access control. At the same time similar systems went online in D.C., Illinois, San Diego, and Tulsa; most of these used barcode technology and electronically read tags attached to

car windows. Monthly bills were sent out in itemized statements listing the place and time of each toll crossing. The total number of drivers involved in these experiments was minimal.

Then Washington, Boston, and New York City's Metropolitan Transportation Authority all joined to create one giant, integrated e-toll system that would eventually cover the Northeast and Mid-Atlantic States as well as parts of Appalachia. The first piece of the system went up in 1989 on New York's Verrazano Bridge, which at the time carried approximately 58 million vehicles a year between Staten Island and Brooklyn. Each vehicle involved in the project received a small box bearing a unique serial number of up to twenty digits that would be read as it passed through tollbooths. The technical knowhow and logistics were handled by the defense contractor Lockheed and communications giant AT&T.[47]

Next, the Lincoln Tunnel was outfitted; using tagged buses and guinea pig trucking companies. From this emerged a commitment from the New Jersey Turnpike, the New Jersey State Highway Authority, and the New York State Thruway Authority to create a coordinated, area wide automatic vehicle identification system that came to be known as E-Z Pass.

Once the Big Apple started tagging vehicles, other started following suite. By the end of the decade numerous state and regional systems cropped up: California had FasTrak; Illinois, I-Pass; Kansas, K-Tag; Oklahoma, PikePassl Virginia, Smart Tag; in Florida they use the SunPass. Honk Kong just calls their high-tech toll tags the "Octopus

Card." Parenti humorously speculates that maybe when all the systems in the United States are linked we might call ours the "Leviathan Card."[48]

By the early 1990s, the E-ZPass system (the largest network of its kind in the world) operating in and around New York City had pulled in eight states: south to Maryland, Delaware, and West Virginia; north to Massachusetts and soon New Hampshire; and west to Pennsylvania. Soon E-ZPass traffic accounted for an estimated 40 percent of all toll transactions and 67 percent of all toll revenue in the United States.[49] In 1993 when the New York system went online publicly 60,000 tags were issued. Within five years that number had grown by a factor of ten; Massachusetts alone had almost a quarter of a million vehicles with E-ZPass tags on its roads. Throughout its area of operation there are now well over two million drivers with E-ZPass transponders in their vehicles. System administrators speculate that two-thirds to all local commuters will eventually be tagged.

The convenience of this system creates a fast-moving toll system for almost the entire East Coast and every other patch of metropolitan sprawl. But behind this convenience lies an incredible machinery of surveillance. Each E-ZPass tollbooth is equipped with a computer, connected by fiber optic cable to a data center in Secaucus, New Jersey, run by Chase Manhattan Bank. Each tag produces a precisely itemized monthly statement that reveals a billing address, credit-card number, how often a driver is on the road, and his or her whereabouts at a certain time. Without much discussion, a system of soft, unstaffed electronic checkpoints has been erected along thousands of miles of highway and at dozens of major urban bridges and tunnels controlling access to some of the nation's most populous cities. We have opted in to a system of unparalleled

convenience; a system of detailed surveillance that logs the movements of millions of drivers. Systems such as these have also been employed for traffic monitoring and management, and even for subway and bus transportation.

Municipal and statewide travels are not alone though where systems of tracking the movements of people are concerned. Some of the most advanced systems of tracking integrate many of the fore mentioned technologies and are employed in the industry of air travel. These systems are installed under the guise of convenience in our increasingly crowded and secured air terminals, but also represent the pinnacle of surveillance technology today.

Since the events of 9/11 air travel has been subject to increasing security measures, often causing long lines and delays as travelers are ushered through intensive security checkpoints. The privately held New York based company, "with experience handling Security Sensitive Information for the Department of Homeland Security, Customs and Border Patrol, Immigration and Customs Enforcement, the Department of Defense, among other government agencies," Verified Identity Pass, has worked out a solution to these lines and delays by introducing the Clear Card. The Clear Card is a form of identification card that employs several layers of surveillance and security technology including embedded microchips, photo images, and biometric information. The card uses the embedded microchip to store your biometric fingerprint and iris image data, as well as other biographical data. This data is used by a terminal to verify your ID and allow access to the benefits of the subscription service. Benefits that are touted as: Fast passage through airport security, access to a designated Clear security lane staffed by professional, courteous Clear attendants, extraordinary customer service, fewer missed

flights, and a stress-free, predictable airport experience. As a registered traveler program it is authorized and regulated by the airports in which it operates, and by the U.S. Government's Transportation Security Administration. The TSA actively monitors the Clear card database and screens all members of the program; they even hold the power to revoke a member's status without notification, upon which the user receives a prorated reimbursement of their membership fees. "Clear" is the first branded consumer product in what V.I.P. calls the "voluntary identity credentialing industry."[50]

As one can imagine, the same personal information that is connected to the E-ZPass system is easily associated with the Clear card system. Though the Clear system goes a step further. The participants opt in to the convenience of easing through airport security by relinquishing their credit card data for payment, and biographical and biometric data for credentialing. This emerging "voluntary identity credentialing industry" is bound to create an active connection between the data collected by commercial and governmental systems of surveillance, bringing with it a whole new era of real-time demographic and personal data available for analyzing that includes how we are, where we are, when we're there, what we're doing or purchasing. A system in which people voluntarily opt in , all in the name of security and convenience.

Conclusions

As one can see by analyzing the history of these surveillance technologies the industry of surveillance has made a marked shift in application since its origins in the

disciplining of subjected human beings. A shift from imposing discipline as a centralized, overtly visible system such as the Panopticon, to a distributed, and at times invisible, system of voluntary, and involuntary, registration where participants are awash in the benefits of the conveniences, information, and security provided by the new surveillance.

Like much of the histories of surveillance technologies, the Foucauldian model of control, and consequently its explanatory power, *refers to the past* and is not concerned with the emergence of the contemporary postindustrial subject.[51] Indeed many have argued that the Panopticon is not necessarily the best possible metaphor to be used in analyzing contemporary surveillance.[52] Gary Marx is one of these theorists seeking to redefine surveillance in the contemporary technological environment.

> "The ratio between what could be known given the means for discovering personal information and what is actually known was probably much smaller in the 19th century than is the case today and was much smaller still in the middle ages and throughout most of recorded human history. The weakness of the technology was matched by the fact that there was much less to be known about behavior.
>
> In absolute terms, given ways of living and comparing pre-industrial, industrializing and contemporary societies, the amount of personal information that is potentially knowable would seem to have increased markedly over time as societal scale, density, differentiation and formal record keeping increased (e.g.: remote communications, the number of people interacted with,

geographical mobility etc.)"[53]

Marx seeks to break from this traditional Foucauldian model of surveillance and argues for a new definition of surveillance other than that of "close observation, especially of a suspected person." He builds his new definition around present revolutions in technology that allow the extraction or creation of personal data. In fact Marx notes that "a better definition of the new surveillance is the use of technical means to extract or create personal data."[54] This "new surveillance" relative to traditional surveillance extends the senses and has a low or nonexistent level of visibility, is more likely involuntary, and integrated into routine activity. The data from this new form of surveillance is available in real time and can continuously offer information on the past, present, and speculative futures.

This new surveillance with its low visibility, involuntary nature, remoteness and lower costs has the clearest social implications. In extending the senses they challenge the fundamental assumptions about personal and social borders, which have been maintained by values and norms and social organization as well as the limits of technology to cross them.

Today in the United States surveillance technology is widely available to the public. A common transmission process is from military to law enforcement to commercial industry to the civilian population. Examples of this can be seen in the proliferation of night vision and GPS technology, drug testing, and the Internet. Marx

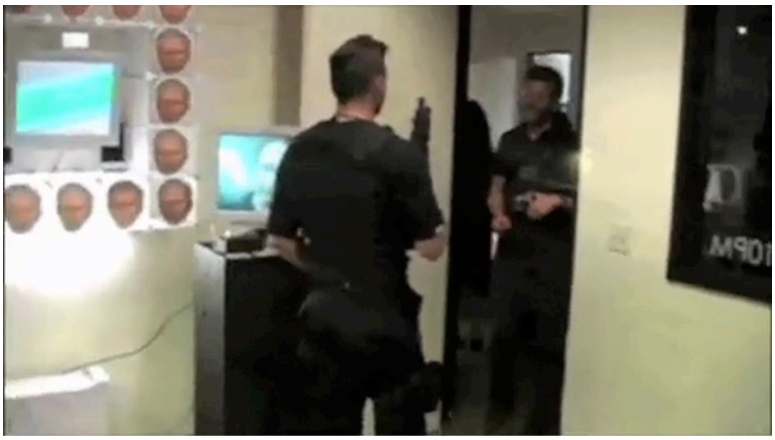
postulates that because of this the new surveillance may move from being a one-way mirror to being a window.

This recent proliferation of surveillance technology has allowed for a creative engagement of surveillance by those that even have little, or nothing, to do with established institutes or agencies employing these technologies. The trickle down nature of technology has reached a juncture where artists are now able to grapple with the nature of surveillance outside of literary and sociological circles. Artists such as Julia Scher, Ann-Sofi Sidén, Christian Moeller, and Wafaa Bilal all appropriate surveillance technologies in their works to inspire questions concerning themes of privacy, control, and even participation in Bilal's case. Though the installation piece that accompanies this paper, "Small Sacrifices," engages the same theme of surveillance, it seeks to break from the common conspiratorial and paranoia-inducing notions of surveillance to incorporate perceived benefits for involvement in the emerging and contemporary societies of surveillance.

"Small Sacrifices" was a time specific performance and installation piece by the Secure Media Access Group (SMAG), revolving around the themes of contemporary surveillance, security, and participation. "Small Sacrifices" was installed for the 2008 University of California Santa Cruz, Digital Art and New Media Masters in Fine Arts show title "Bureau of Disruptions." The piece implored gallery visitors to participate in an abstracted version of the current surveillance society where opting in to the system allowed for the purchase of benefits provided by new surveillance technology.

View from outside the PSC. SMAG Administration Agent collecting information and participants viewing products and commercials.

The installation consisted of SMAG's Personal Security Center (PSC), a membership only shopping center, where participants were given the chance to purchase objects that would increase their security and secure their status as non-threats. In order to access these benefits though participants were required to submit their names, email addresses, and a facial image. In exchange they were issued an RFID enabled membership card marked with the SMAG logo. The facial image taken of a given participant was tied to the numerical data on their membership card and allowed for a guard to visually compare the image to the gallery visitor attempting to enter the Personal Security Center.



SMAG Guard checking membership cards at the PSC entrance.
Specifically denying access to a participant
that does not have a matching card.

This guard, stationed at the only entrance and exit for the installation, controlled access to the Personal Security Center by visually checking the identity of those attempting to enter. The SMAG Guard would scan a member's RFID card and if their person matched the facial image submitted upon registration they were allowed to circumvent the control of the security personnel and enter the store. Those with stolen, or no membership cards, were asked to step out of line and return to the agent issuing membership cards. Many gallery visitors, upon later questioning, expressed being threatened by the presence of the fully armed guard, opted to remain outside the PSC and were left to watch what was going on inside through windows running down one wall. On a few occasions when the SMAG Administration Agent was absent the installation even went into full lockdown with the guard denying access even to those with valid membership.

This interaction and circumvention of control through participation was only a piece of the puzzle that "Small Sacrifices" presented. Once inside members were confronted with display units exhibiting several surveillance related products available

for purchase. In order to purchase the following products, participants were required to submit biometric information including fingerprints, voice samples, and DNA samples. These products included a “Home Terrorist DNA Test,” a “Terrorist Panic Button,” and a “Digital Camo Facemask.” These products were each accompanied by video displays looping their individual commercials. Each of these artifacts and their commercials were designed to offer a questionable sense of security to the purchaser.

Products and commercial displays.
Top Left: Terrorist Panic button
Bottom Left: Digital Camo Face Mask
Right: Home Terrorist DNA Testing Kit

The first of these products, a “Home Terrorist DNA Testing Kit,” available for the low price of two voice samples, offered a way to test yourself or someone you are close with for their perceived terrorist threat level. It was also stated that the Department of Homeland Security monitored all results of the DNA testing. This DNA test and commercial offered a tongue in cheek engagement with notions of paranoia and security in contemporary society. The next product, the “Terrorist Panic Button,” was a black box with a large red button that read “Terrorist Alert” and available for the cost of a set of five fingerprints. The rear of the box noted that the button was GPS enabled and should be depressed when the participant was witness to a supposed terrorist or terrorist event.

This button made of paper and with vague descriptions of what happens when you press, was meant to engage notions of futility and obscurity in many surveillance and security practices. The "Digital Camo Face Mask," by far the most expensive at the price of a DNA sample, was designed for the participant to wear in order to bypass facial recognition software scanning for terrorist threats. The mask consisted of a pixilated portrait of George W. Bush, U.S. President during the 9/11 attacks and declarer of the global war on terrorism. This mask was meant to engage the nature of circumventing security technology and procedures by the act of voluntarily submitting information that guarantees security status and participation in an ever-increasing state of threat. Most of the participants that purchased the mask were mainly concerned with how the DNA information is used and questioned the SMAG Administration Agent on the Group's policies. The response was that the information was kept secure and only shared with the Department of Homeland Security in order to verify threat level and document those who are issued the "pass" that allowed them to bypass facial recognition.

In all the installation, by participant response, seemed to successfully engage the modes and ideas of contemporary surveillance, participation, security, and the circumvention of traditional forms of control and power, to offer a critique of the emerging surveillance society. Many participants offered their observations on the installation and their responses dictated that the ideas behind it were communicated effectively and inspired them to question the "opt in" nature of today's surveillance practices. One of the most notable responses to the project was that of an almost classically nuclear family that opted to participate in the PSC. The family consisted of a father, mother, and three children, which each submitted information to receive their

individual membership cards, and subsequently spent a large block of time viewing, discussing, purchasing, and questioning the products and commercials. Their discussions as overheard by the SMAG Administration Agents touched on many of the themes addressed in the piece, with the adults even explaining to the younger how the processes of the installation relate to their activities on the Internet and social networking sites. The model of the installation's engagement with current topics and its breaking with traditional critiques of surveillance proved successful in communicating the issues revolving around the emerging surveillance society.

The downfall with many other current critical artistic, and literary, engagements of surveillance, from governmental to commercial, is that the main issues addressed stem from the roots of technology used for state control and discipline. With a past so involved literally in the commoditized human and the pursuit of criminals it is understandably difficult for some to separate the past and present to focus on the beneficial aspects of surveillance technologies that extend beyond the scope of populace management into individual security, mobility, personal safety and convenience. These benefits are largely due to the advances in surveillance technology, its increasing availability, and its migration from systems used to catch and discipline individuals after a transgression of the law to systems designed to actively monitor, inform, protect, and increase convenience in real time.

End Notes:

---

[1] Michel Foucault, *Discipline and Punish: The Birth of the Prison*. (New York: Pantheon,1977), 172,176.

[2] Foucault, 201.

[3] Foucault, 205.

[4] Foucault, 200.

[5] Christian Parenti, *Soft Cage: Surveillance in America From Slavery to the War on Terror*.(New York: Basic Books, 2003), 15.

[6] Parenti, 14-15

[7] Parenti, 19.

[8] Parenti, 19.

[9] Parenti, 17.

[10] Parenti, 25.

[11] Parenti, 29.

[12] Parenti, 31.

[13] Parenti, 32.

[14] Parenti, 35.

[15] Parenti, 38.

[16] Parenti, 41.

[17] Parenti, 42.

[18] Parenti, 42.

[19] Parenti, 42.

[20] Parenti, 46.

[21] Parenti, 47.

[22] Parenti, 47.

[23] Parenti, 49-50.

[24] Parenti, 50.

[25] Morton, David. "Recordings and the 'surveillance society' *Recording History: The History of Recording Technology*. (2006), http://www.recording-history.org/HTML/surveillance1.php

[26] Nieto, Marcus, et al., "Public and Private Applications of Video Surveillance and Biometric Technologies." California Research Bureau. (2002), http://www.library.ca.gov/crb/02/06/02-006.pdf

[27] Parenti**,** 109.

[28] Parenti, 117.

[29] Parenti, 78.

[30] Parenti, 79.

[31] Parenti , 78.

[32] Parenti , 79.

[33] Parenti , 80.

[34] Parenti , 81.

[35] Parenti , 86.

[36] Parenti , 87.

[37] Parenti , 89.

[38] Parenti , 89.

[39] Parenti , 92.

[40] Parenti , 95.

[41] Parenti , 95.

[42] Parenti , 95.

[43] Parenti , 99.

[44] Parenti , 100.

[45] Parenti ,102.

[46] Parenti ,106.

[47] Parenti ,123.

[48] Parenti ,124.

[49] Parenti ,124.

[50] Verified Identity Pass, Inc. 2008. “Clear - Frequently Asked Questions About Airport Security Fast Pass.” 2008. http://www.FlyClear.com/.

[51] Lianos, Michalis. "Social Control after Foucault." Surveillance & Society, Volume 1 Number 3 (2003), http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf

[52] Koskela, Hille. "'Cam Era' - The Contemporary Urban Panopticon." Surveillance & Society, Volume 1 Number 3 (2003), http://www.surveillance-and-society.org/articles1(3)/camera.pdf

[53] Marx, Gary. "What's New About the "New Surveillance"? Classifying for Change and Continuity." Surveillance & Society, Volume 1 Number 1 (1 September 2002), 23. http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/50/50

[54] Marx, 11.

Bibliography

Ball, Kristie. “Organization, surveillance and the body: towards a politics of resistance.” *Theorizing Surveillance: The Panopticon and Beyond*. Edited by David Lyon. Cullompton, Devon: Willan Publishing, 2006.

Bogard, William. “Surveillance Assemblages and Lines of Flight.” *Theorizing Surveillance: The Panopticon and Beyond*. Edited by David Lyon. Cullompton, Devon: Willan Publishing, 2006.

Fleck, Robert. “Who Told the Chambermaid” *Venice Biennial* pp. 182, La *Biennale di Venezia 48a Esposizione Internazionale d´Arte, dAPERTutto*. (1999) http://www.crac.org/htmls/siden.html

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Pantheon, 1977.

Gandy, Oscar Jr. . “Data Mining, Surveillance, and Discrimintation in the Post-9/11 Environment.” *The New Politcs of Surveillance and Visibility*. Edited by Kevin D. Haggerty & Richard V. Ericson. Toronto: University of Toronto Press, 2006.

Gilliom, John. “Struggling with Surveillance: Resistance, Consciousness, and Identity.” *The New Politcs of Surveillance and Visibility*. Edited by Kevin D. Haggerty & Richard V. Ericson. Toronto: University of Toronto Press, 2006.

Haggerty, Kevin D. and Richard V Ericson. *The New Politcs of Surveillance and Visibility*. Edited by Kevin D. Haggerty & Richard V. Ericson. Toronto: University of Toronto Press, 2006.

Hultkrans, Andrew "Danger dirty data - technology in the art of Julia Scher". *ArtForum*. (September, 1995) FindArticles.com. http://findarticles.com/p/articles/mi_m0268/is_n1_v34/ai_17501983 (Accessed: 20 March, 2008).

Koskela, Hille. "'Cam Era' - The Contemporary Urban Panopticon." *Surveillance & Society*, Volume 1 Number 3 (2003), http://www.surveillance-and-society.org/articles1(3)/camera.pdf

Lianos, Michalis. "Social Control after Foucault." *Surveillance & Society*, Volume 1 Number 3 (2003), http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf

Lyon, David. *Surveillance After September 11 (Themes for the 21st Century).* Cambridge: Polity, 2003..

Lyon,David. *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination.* London: Routledge, 2003.

Lyon David, ed., *Surveillance Studies: An Overview*. Cambridge: Polity, 2007.

Lyon, David, ed., *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton, Devon: Willan Publishing, 2006.

Marx, Gary. "What's New About the "New Surveillance"? Classifying for Change and Continuity." *Surveillance & Society*, Volume 1 Number 1 (1 September 2002), http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/50/50

Marx, Gary. "Varieties of Personal Information as Influences on Attitudes towards Surveillance." *The New Politics of Surveillance and Visibility*. Edited by Kevin D. Haggerty & Richard V. Ericson. Toronto: University of Toronto Press, 2006. (also available at garymarx.net)

Marx, Karl. *Das Kapital.* Edited by Fredrick Engels, Translated by Samuel Moore and Edward Aveling. Moscow: Progress Publishers, 1887. http://www.marxists.org/archive/marx/works/1867-c1/index.htm

Morton, David. "Recordings and the 'surveillance society' *Recording History: The History of Recording Technology*. 2006. http://www.recording-history.org/HTML/surveillance1.php

Nieto, Marcus, Kimberly Johnston-Dodds, and Charlene Wear Simmons Ph.D. "Public and Private Applications of Video Surveillance and Biometric Technologies." *California Research Bureau*. (2002) http://www.library.ca.gov/crb/02/06/02-006.pdf

Ogura, Toshimaru. "Electronic Government and Surveillance-Oriented Society." *Theorizing Surveillance: The Panopticon and Beyond*. Edited by David Lyon. Cullompton, Devon: Willan Publishing, 2006.

Osborn, Barbara. "APPREHENDED: JULIA SCHER OCCUPATION: ARTIST" Interview for *Adaweb*. http://adaweb.walkerart.org/~purple/scher.html

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

Roberts, Lucy. "The History of Video Surveillance - From VCR's to Eyes in the Sky." *Video Surveillance Guide*. 2005. http://www.video-surveillance-guide.com/history-of- video-surveillance.htm

Stalder, Felix and David Lyon. "Electronic identity cards and social classification." *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination.* Edited by David Lyon. London: Routledge, 2002.

Turow, Joseph. "Cracking the Consumer Code: Advertisers, Anxiety, and Surveillance in the Digital Age." *The New Politics of Surveillance and Visibility*. Edited by Kevin D. Haggerty & Richard V. Ericson. Toronto: University of Toronto Press, 2006.

United States Department of State. "U.S. Passport Card." http://www.travel.state.gov/passport/ppt_card/ppt_card_3926.html

Van Der Ploeg, Irma. "Biometrics and the body as information: normative issues of the socio-technical coding of the body." *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination*. Edited by David Lyon. London: Routledge, 2003.

Verified Identity Pass, Inc. 2008. "Clear - Frequently Asked Questions About Airport Security Fast Pass." 2008. http://www.FlyClear.com/.

Wall, David S. "Surveillant Internet Technologies and the Growth in Information Capitalism: Spams and Public Trust in the Information Society." *The New Politics of Surveillance and Visibility*. Edited by Kevin D. Haggerty & Richard V. Ericson. Toronto: University of Toronto Press, 2006.