Against Data Determinism in a Networked World
Brooke Singer, Spring 2002

Contact: bsinger@bsing.net

Table of Contents

Abstract

The current trend to collect all data on all people has resulted in a phenomenon called the data-self. This data doppelganger is not an explicit self or even a tangible self, but has real consequences on our everyday lives. As our data-selves have become more defined, accessible, and trusted, more and more decisions are made based on these virtual stand-ins without any notification or much awareness by the subject. Due to the growth of computer technologies and networked systems, data determines how we live, who we are, and what opportunities we are allowed more than ever before.

Privacy advocates form the most vocal and organized group addressing the issues surrounding personal-data collection. While privacy advocates have made important differences, there are other ways to frame data-collection issues. Sociologists, for instance, shift the focus from an individual concern toward larger questions of social justice. Artists, also entering the data-collection discussion, are in a unique position to promote understanding and debate. A technologically oriented art practice is, furthermore, capable of temporarily breaking the tight grip of data surveillance to initiate openings for public response and resistance.

Part One: The Data-Self, the Database, and Social Orchestration

Introduction

My investigation into the digital-self began two years ago with questions concerning my online persona: How accessible am I on the web? What kind of information is out there? What does it look like? And how do I appear in a digitized and dispersed form? It was a narcissistic concern more than anything else. I was spending hours participating in online user groups to get technical support for software and was keenly aware of others and myself in such a detached yet seemingly intimate forum. I remember being so moved by the help of one anonymous individual that I sent digital flowers (or an image of flowers I captured with my video camera) to this person as a "thank you" (see fig. 1).

As my participation in online communities increased, my curiosity grew stronger. I began to wonder how to piece these people together from their email postings in conjunction with any random assortment of online materials that I could find. After a few hours of research, I realized how easy it is to find information about people online. I was able to get information like date of birth, voter registration data, real estate holdings, salaries, marriage licenses, birth records, and demographic statistics with a few clicks of my mouse. As I was attempting to piece others together, I wondered if and how I was being similarly assembled.

I did not see my online interactions purely as the joyous, experimental play-spaces Sherrie Turkle describes in Life on the Screen: Identity in the Age of the Internet. In this book from the mid-1990s, Turkle voices unbounded enthusiasm for the Internet, an enthusiasm prevalent at the time. For Turkle, online interactions are an opportunity to liberate the rigidly proscribed, modernist self in favor of a fluid, non-linear and schizoid self. She writes in this book:

> In my computer-mediated worlds, the self is multiple, fluid, and constituted in interaction with machine connections…. And in the machine generated world of MUDs [multiple user domains], I meet characters who put me in a new relationship with my own identity…. In such ways, MUDs are evocative objects for thinking about human identity and, more generally, about a set of ideas that have come to be known as 'postmodern' (15-17).

Turkle found agency in her online forums. These were productive and empowering territories in which she could experiment with her identity and its construction. In contrast, my online experiences gave me reason to pause. I came to see my cyber persona as not fully knowable and not in my control. The schism between it and myself did not seem like one to necessarily celebrate. For me, play and interpretation were overshadowed by the potential for gross misuse. My curiosity turned into concern. If my digital-self were remote, not fully knowable and not in my control, then the risk for abuse seemed high.

But why does this digital-self matter? What is the risk? And what exactly is the digital-self? These were my initial questions directing my research and eventually redirecting my art practice.

Terminology

The digital-self is any digitally encoded information that describes me or is associated with me. This includes my emails, my home page, my holiday snapshots scanned into Photoshop, search engine results for my name, Amazon.com recommendations for me based on my shopping patterns, my jpeg image and bio on my company's web site and so forth. It is a mixture of materials I actively create and view along with materials created by others of which I may or may not be aware.

A subcategory of the digital-self, and the primary focus for this paper, is the data-self. This, too, is digitally encoded but specifically to interface with a database. My data-self accumulates as byproduct from my interactions in the physical and virtual worlds. Every time I use a credit card, surf the web, talk on my cell phone, visit the doctor, and register to vote, for instance, I trigger a stream of data. This stream of data is sometimes referred to as a data-wake. The term data-wake implies the data follows me and is a passive residual of my physical body. I would argue, however, that this data in time precedes my

body and can have more importance than my physical self. My data-self determines if I get a loan, a job or health insurance. And it is increasingly put to other uses as my data-self becomes more accessible, defined, and trusted.

The data-self, therefore, is composed of fragments of my data-wake that are pieced together, analyzed and used by others (mostly by corporations and the government) for purposes like market research, security assurance, event coordination and authorization. My data-self is not an aggregate of my data wake since databases are far too numerous and are not yet linked or centralized. Rather, select bits are abstracted from my life to create my virtual stand-in.

This distinction between the digital-self and the data-self is mine. I use it primarily to distinguish a general digital representation of the self from a more specifically structured and refined data-self. This structure or syntax of the data-self is important; it allows the data-self to flow into and between various databases with minimal resistance. Standardization through code enables liquid networks in which the exchange of data is possible and use-value is optimized. Terms like data-body, data-image or data-subject are used by other writers to connote similar ideas (Lyon, The Electronic Eye 41; Poster, The Information Subject).

Privacy

My interest in the data-self led me first to the privacy camp. Today there is an active, global community, particularly online, that organizes itself around and adamantly defends an individual's right to privacy. Privacy groups contend that what I call the data-self should not be controlled by government and corporate interests, but rather individuals are the rightful owners of their own data. Only the individual should decide if and what personal data is collected, when it can be used, and under what circumstances.

In recent years, privacy rights have become a hot topic thanks to the rise of personal computing and the telecommunications industry. Privacy concerns, of course, existed before computers. The right to privacy is not explicitly outlined in the U.S. Constitution, although many have interpreted the First, Fourth and Fifth Amendments to include them (Goldhamer, par.2). The legal concept of privacy was first established in 1890 with a now famous law-review article written by Louis D. Brandeis and Samuel D. Warren. They wrote:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual…the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops" (Warren and Brandeis 193).

It is no coincidence that Warren and Brandeis wrote their review when they did. With the advent of photography, and more importantly the dissemination of photography in daily newspapers, the time had come for privacy to become a documented, legal issue. The very nature of public space versus private was called into serious question by new technologies.

Warren and Brandeis' review not only established a person's right to privacy (the right "to be let alone"), but it was also a shift in the privacy paradigm. Traditional notions of privacy concerned one's physical body or territory. Warren and Brandeis, however, recognized the need to expand privacy rights to defend a person's immaterial territory, their photographic image. Today the word privacy more often than not is referencing data protection (a term used in Europe and perhaps a more useful one). It does not automatically imply the older, physical protections. This is most likely because the "physical" right to privacy has been naturalized; it is understood and assumed. The issues of data privacy, however, are not.

The Privacy Journal, a print newsletter and online web site devoted to privacy matters, defines the present-day use of the word privacy as "the right of individuals to control the collection and use of personal information about themselves" (Privacy Journal). Privacilla.org, an online resource for privacy protection, explains its privacy position this way: "A person has privacy when two factors are in place. He or she must have the ability to control information

about him- or herself, and he or she must exercise that control consistent with his or her values" (Privacilla, par. 1).

These two quotations illustrate the present-day emphasis on privacy as an information concern and privacy as an individual consideration based on personal values. There is also a strong emphasis on individual action; participation by the public to take control over their data is considered a necessity for change to occur.

But is the public equipped to deal with privacy issues? Polls show privacy is a major concern for people, but behavior does not support this. In a Pew Internet Project report conducted in August 2000, researchers found that "Online Americans have great concerns about breaches of privacy, while at the same time they do a striking number of intimate and trusting things on the Internet…" (Pew, par.2). The Pew research also found that more than half of Internet users could not identify the most basic, online, data collecting tool: the cookie (Electronic Privacy Information Center, par.10). With government regulation lacking and industry self-regulation highly suspect, privacy advocacy groups fill the important role of educating and mobilizing the public. Some of the more respected and popular privacy groups are the Electronic Privacy Information Center (EPIC), Electronic Frontier Foundation (EFF), Center Democracy and Technology (CDT), Computer Professionals for Social Responsibility (CPSR), Privacy Foundation and Privacy International.

The following discussion of privacy groups focuses primarily on Internet usage, but the Internet is only one aspect of the privacy issue. While the Internet makes data collection and data profiling techniques more transparent, the real abuses are most likely in private databases that are password protected and away from public scrutiny. As one privacy advocate, Robert Ellis Smith, stated: “[People] are truly awed by the information that is collected on the Internet and the tricks that can be done with it. I still think that the major threats are probably offline and I would hate to see too much attention given to Internet privacy. I think that offline problems are as great” (Privacy Foundation, par. 13).

Online practices offer a way into the discussion of data collection and data usage since the web is so accessible. While these practices may not be the worst-case scenarios or the complete picture, they give a good indication of current data trends.

Privacy Advocates: What are they doing and saying?

The most obvious gain by privacy advocacy groups online is the ever-present privacy policy page. Major businesses, and all businesses involved in e-commerce, have links to their privacy policy in order to gain public trust and, hence, more business. Such postings are not required by law, but are

nonetheless ubiquitous. Privacy groups originally pressed for these pages and now closely monitor them (Junkbusters, par.10). The threat of federal regulation of these policies has further encouraged the business world to comply.

Advocacy groups may be pleased with the quantity of these online privacy policies, but the quality is a different matter. Online privacy policies are often criticized for being too long and too convoluted. Making sense of the fine print is troublesome and time consuming, even for an expert. Also privacy policies on company web sites can change day to day with little or no warning. And, most importantly, there is no standard; exactly what is protected and how well varies dramatically.

Many advocates are pushing for a standard online privacy policy for businesses and many, like Robert Ellis Smith, look toward the Code of Fair Information Practices for guidance. This code would enforce “Notice, Choice, Access and Security” whenever data collection takes place (Federal Trade Commission, par.3). Smith states, “A lot of companies will subscribe to a couple of points but not the whole thing. The main principle is that you don't use information for a purpose that's different from the purpose you gathered it, unless you get the consent of the individual” (Privacy Foundation, par.27).

In May 2000, the Federal Trade Commission recommended the implementation of a standard Internet privacy policy to protect consumer privacy online despite strong support for industry self-regulation by politicians and business leaders alike. The FTC made this endorsement because it found that not even a minimum level of privacy protection was in place on many web sites. The report states:

> The results showed that only 20 percent of the random sample sites were found to have implemented all four fair information practices [of Notice, Choice, Access, and Security]. And among the most popular group, only 42 percent did so. Even when the report looked at the percentage of sites implementing the two critical practices of Notice and Choice, only 41 percent of the random sample and 60 percent of the most popular sites provided such privacy disclosures (Federal Trade Commission, par. 4).

Two years after the FTC's recommendation, however, there is still no standard online privacy policy required by law. Politicians are not pushing forward on federal regulation of personal data collection practices and this is not just a matter of laissez-faire politics. In Jeffrey Rosen's insightful article "Silicon Valley's Spy Game" appearing in the *New York Times Magazine* on April 14th, 2002, the author states that politicians are not up to the task. Rosen describes one technologically savvy Congresswoman, Maria Cantwell, who advocates privacy laws, as "pessimistic that her colleagues in Congress have the understanding or inclination to regulate technology in a meaningful way" (Rosen 51).

Privacy advocates were successful in moving the government to act and stopping a company from going back on its privacy promise in the case of DoubleClick. DoubleClick, an online advertising company, purchased an offline direct marketing company, Abacus, for $1 billion in 1999. When DoubleClick announced its plans in January 2000 to merge its online data with their newly-acquired offline information, privacy advocates balked. Combining online surfing records with detailed personal records collected separately offline smacked of unfair business practice. In addition, DoubleClick would have had to reverse its privacy policy in order to make this data merger. DoubleClick's privacy policy clearly stated—and still states today—that information collected on Internet users is kept anonymous.

In response, the Electronic Privacy Information Center (EPIC), a privacy advocacy group, filed a complaint with the FTC, accusing DoubleClick of unfair and deceptive trade practices and demanding an investigation. The FTC initiated an investigation and soon afterwards DoubleClick's CEO, Kevin O'Connor, announced that "[he had] made a mistake by planning to merge names with anonymous user activity across Web sites in the absence of government and industry privacy standards"(Tech Law Journal, par.4). The program was withdrawn and DoubleClick survived the negative publicity.

Political and legal action, of course, are not the only method of resistance. There are numerous software solutions that protect individuals against invasion of privacy, and many of the online advocacy groups advertise them. The Privacy Foundation offers “Bugnosis,” a web bug detector. Web bugs are invisible images on web pages that can transfer information about the web surfer or transfer information the web surfer inputs into a form to a another, undisclosed location. Prior to Bugnosis, only programmers could detect web bugs by reading a site’s source code. Bugnosis makes web bugs visible to all.

Other examples of technological resistance to online personal data collection include the Anonymizer (software that allows you to anonymously surf the web) and HushMail (free, web-based email that uses encryption). The problem with technological fixes, however, is that they favor the group that needs them least, the technologically elite. A person must understand the technology enough to identify the problem in the first place and then be able to use the technological fix correctly in order to gain protection. Such technological Band-Aids do not usually help the average, everyday user.

What’s the Matter with Privacy?

While the privacy camp is the most active and effective community discussing data collection and usage, there are other useful ways to frame the issue. Robert Ellis Smith believes the general “privacy way” concedes too much. He

poses an interesting question: Should we be collecting personal data in the first place? Privacy advocates usually focus attention on how to limit personal data usage or pare down data so it is rendered anonymous. “At some point we ought to think about whether it is appropriate to even gather the information,” Smith states. “The debate is not there right now” (Privacy Foundation, par.20).

The debate is not there because personal data collection has a long history that is rooted in the most basic Western ideal—democracy. Democracy is based on a belief in the value of the individual. Each citizen becomes accountable and, therefore, countable to ensure the rights of democracy (one person, one vote) and some sort of record keeping is put in place. As a society grows, so does its recording system (or bureaucracy). If records are not destroyed, what is originally collected to maintain democratic rights can be reused for altogether different purposes. The question is whether data can be collected for the social good and not be reused later, resulting in social detriment.

A current example of a social good gone wrong is the Social Security Act and its creation, the Social Security Number. After the Great Depression in 1935, President Franklin D. Roosevelt proposed to Congress economic-security legislation that resulted in the Social Security Act. To keep track of the new social benefits, Congress established the Social Security Number. Initially,

President Roosevelt declared this number would be used solely for the purpose of Social Security to deter any fear of a national identification number. For the first few decades, in fact, there was a warning on Social Security cards that read: "Not to be used for Identification" (Hibbert, par. 7).

No law, however, protected Social Security Numbers from becoming a form of identification or verification. And by 1961, the Internal Revenue Service was employing the Social Security Number for identifying taxpayers. Today Social Security, the IRS and state departments of motor vehicles can all lawfully utilize the Social Security Number (American Civil Liberties Union, par. 3). Numerous other government agencies and commercial businesses request the number as well, though compliance is supposedly voluntary.

The Social Security Number, originally established for social benefit, has become a de facto national identification number. When providing this number, a person unlocks a barrage of personal information. Medical data, financial records, driving records, education records, to name just a few, are often linked to this nine-digit number. A Social Security Number is useful because—unlike a name, address or date of birth—it is unique and fixed from birth until death. Because of its extensive use, this one number can create a vivid picture of a person. Thus, when a Social Security Number is handed over to a business or government organization, a person is contributing to his or her ever-growing, life-long data file. In addition, the organizations receiving

the number can access more information than people usually realize and much more information than is likely necessary. Excess information can, among other things, lead to a prejudiced decision-making process.

Today the extensive use of Social Security Numbers is allowing centralization of personal data. Without a standard method for identifying people, it becomes more difficult to merge databases. Without the Social Security number, bits of personal information are forced into isolation and disuse. The Social Security Number is a guarantee for cross-referencing databases and bringing disparate information into a more powerful whole. It ensures that personal data have longevity. With the Social Security Number, data can withstand the pressures of a fluctuating world and remain forever meaningful.

In the case of Social Security, a social need necessitated the disbursement of benefits and a data-collection system was established to facilitate the job. Other government agencies and businesses soon realized the tremendous potential of the Social Security identifier. Relaxed laws gave way to abuse of the system and a national identification number is now in effect. Can future laws prevent such abuse from happening again or is personal-data collection destined to retaliate against those who initially comply with the system?

Beyond Privacy

While Robert Ellis Smith finds certain questions not addressed by privacy groups, I am discovering something else: most people are already decided on the issue. In response to the word privacy, people will say “how do I protect myself?” or “what do I have to hide?” There seems to be little room for discussion once the “word “ has been spoken. And what discussion there is hardly ever moves beyond an individual’s personal concern for the larger picture—society as a whole.

By reducing the issues of data collection to a matter of privacy, a convoluted and complicated matter is reduced to a single dimension. Legal language dominates and interests are limited mainly to the personal and economic. Discussion around data collection might begin with privacy since our self-interest is most moving to us, but to stop there is short-sighted.

For someone like David Lyon, questions concerning data collecting and the tracking of individuals through data do not culminate in an issue of privacy, but emphasizes social control. The form of social control that most interests Lyon is modern-day surveillance or ‘dataveillance.’ This is “the collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data has been garnered” (Lyon, Surveillance Society 4). Lyon’s research, therefore, centers on issues of surveillance as he considers what it means to live in an information society.

Lyon writes in his book Surveillance Society:

> Concern with privacy can often deflect attention from other aspects of surveillance. Above all, privacy tends to reduce surveillance to an individual matter rather than an inherently social concern. [I see] the question of surveillance…as an issue of sociological interest because it contributes to the very ordering of society (4).

Lyon's sociological perspective shifts the conversation from politics and citizenship to everyday life and society. The data-self is not seen as property to protect, but as a phenomenon propagated by a society that embraces all things digital. As computer-mediated interactions proliferate and become common, participation in modern life has become dataveillance. Surveillance is no longer only relegated to the government nor is it visible by a uniform, watchtower or searchlight. It seamlessly flows as electronic commodity from the public to the private, from businesses to the government, between individuals and groups. We are all implicated through the most mundane tasks like walking down the street, surfing the web, making a phone call, using the local library or going to the doctor.

So what does it mean for us to live in a dataveillance society? How does constant surveillance change the way we live and act? How did we get to this point?

Surveillance is, of course, nothing new or always a bad thing. Dataveillance, as I mentioned before, upholds democratic ideals like the universal right to vote and ensures that people who need welfare receive its benefits. Recently, there has been a call for increased surveillance to fight terrorism. More ordinary benefits of dataveillance include notification of sales that may be of interest to us, fast-lane access at highway tolls, discount prices at grocery stores and assistance with directions when someone is lost.

Because of these benefits, dataveillance is often welcomed and the negative aspects overlooked. It is the price people pay for convenience and security. But many times, dataveillance is misunderstood or not at all apparent. This is due to the invisible and technological nature of modern-day surveillance systems.

Due to its electronic and non-physical nature, dataveillance is subtle. Rarely do we or can we acknowledge its presence, thus allowing dataveillance to exist and expand with little resistance. Lyon writes:

> Most surveillance occurs literally out of sight, in the realm of digital signals. And it happens…not in clandestine, conspiratorial fashion, but in commonplace transactions of shopping, voting, phoning, driving and working. This means that people seldom know that they are subjects of surveillance, or if they know, they are unaware how comprehensive others' knowledge of them actually is (Electronic Eye 5).

Surveillance has been transformed from a tangible thing (i.e., most wanted posters) to abstract code (i.e., data profiling). This transformation has been occurring slowly over centuries, and dataveillance is the newest extreme in the progression towards invisibility.

What is invisible, of course, is either not knowable or easy to forget. Even if dataveillance were open to the public, its code or language is completely incomprehensible to the average person. Only computer experts or the technically savvy can understand such systems and their implications. If you are not one of these people and you ask what is happening, you must trust the answer you are given. Making dataveillance visible would mean making data-collection systems open *and* understandable to the public.

Lyon states that datavellience is not clandestine, but I would disagree. Although surveillance happens in public spaces and directly before us, why is so little effort made to clearly inform the public? Why, for example, are video surveillance cameras usually not marked and why are many cameras made to look like things other than what they are? Why is dataveillance so often "hidden in plain sight" (Camera Surveillance Players, par.3).

The Camera Surveillance Players (CSP) are acutely aware of this problem. The CSP is a New York-based group that stages live performances before surveillance cameras to educate the public about the cameras and resist the

explosion of electronic visual surveillance. In addition to its plays, CSP conducts walking tours in cities to show people where cameras are. It does this to demonstrate how many of these cameras exist and again to educate the public about what cameras can look like and what they can do.

In its literature, the CSP write:

> [V]ery few of the police surveillance cameras in New York are properly labeled. None of them bear signs that warn the passers-by that they are under constant video surveillance by the police. This is very peculiar. If it's true that the cameras have been installed to prevent criminal activity *before* it takes place, rather than simply document it *as* it takes place, then you'd think that big bright warning signs would be the norm, because a criminal is more likely to see and understand the meaning of such a sign than he or she is to see and understand the meaning of a small, globe-shaped object on top of a pole somewhere. The fact that the NYPD's cameras aren't labeled suggests that they weren't in fact installed to prevent criminal activity, but as part of an experiment in the social control of law-abiding citizens, which to be successful requires that the test subjects be unaware of the fact that they are part of an experiment (Camera Surveillance Players, par. 22).

The camera's invisibility, as the CSP argues, ensures compliance, not protection. Dataveillance's invisibility equally fosters compliance. What is protected is the data-collector's interest, not the public interest. The data-collector is enabled to receive valuable personal data with the greatest possible ease.

Recently, I experienced this firsthand when I gave my driver's license to my local liquor store for proof of age. The clerk looked at the date of birth printed on the card *and* swiped the card through a scanner. I was not asked for permission; neither was I told what was happening. I assumed that the scanner was verifying the authenticity of my license.

It was not until I read a *New York Times* article on March 21, 2002, that I understood what had happened. The scanner was reading an electronic strip on the back of my driver's license that holds my personal information. The strip usually contains a person's name, address, date of birth, gender, hair color, height, weight, eye color and sometimes even a Social Security number. I am unsure what information is transmitted when my card is scanned. The card does not indicate how I can find out what information is there or even what the strip's function is. Again, the invisible, stealthy nature of the dataveillance forced compliance and protected the business' desire to gather my personal data.

According to the article in the *New York Times*:

> [A bar owner] bought the [scanner] to keep out underage drinkers who use fake ID's. But he soon found that he could build a database of personal information, providing an intimate perspective on his clientele that can be useful in marketing. "It's not just an ID check," he said. "It's a tool."

> Now, for any given night or hour, he can break down his clientele by sex, age, ZIP code or other characteristics. If he wanted to, he could find out how many blond women named Karen over 5 feet 2 inches came in over a weekend, or how many of his customers have the middle initial M. More practically, he can build mailing lists based on all that data—and keep track of who comes back (Lee, par. 4 - 5).

The article also reported that these strips are utilized in 40 different states and the others are in the process of adopting them. Thirty of the states already implementing the strip are updating the technology to increase its storage capacity and thus the kind of information it can hold. Georgia, for instance, is storing two fingerprints and a signature; Tennessee is equipping its license with face-recognition capabilities; Kentucky is able to store black and white, photographic images on its strip. Liquor stores and bars are not the only places that find these strips handy; hospitals, airports and state legislatures are also putting them to use nationwide.

One quote from the article especially exposes how people do not fully understand the implications of new technologies, even those who are creating them and forcing them into our everyday lives. One manufacturer of the scanning equipment says, "'It's the same information as the front of the license. If I were to go into a bar and they had a photocopier, they could photocopy the license or they could write [the data] down. They are not giving us any information that violates privacy" (Lee, par. 14).

There are obvious differences between using a scanner and photocopier to record the license data. If the clerk had taken my license and put it onto a Xerox machine, I would know exactly what was occurring and would have had the means and time to protest. Furthermore, a reproduction of my license is a far cry from digitizing the information and dumping it directly into a store-owned database. Of course, the store could later manually enter the license information into a data system from the photocopy, but this would be time-consuming and labor-intensive. A significant deterrent would be in place. With scanning machines a database is developed fast, cheap and out of sight. It is a total force that can turn all customers into data material through one simple swipe. It is a background event that happens without public permission or even notification.

So what is done with all of this data and why is it so valuable? For businesses, as the newspaper quote suggests, the major benefits are market research and consumer targeting. Profiling customers and tracking consumer habits allows a business to streamline operations so there is less waste and more return. More bang for the buck in laypersons' terms. Advertisements can be sent to the most appropriate customers and products are tailored quickly in response to data trends. This data can also be very convincing; financial backers like to see proof before committing funds and businesses can find that proof in the numbers. Information, like that gathered from the

license strip (name, address, age, gender), is a gold mine for a business, especially when it is obtained free of charge.

There are other less traditional ways businesses are using personal data they collect. Last year in Connecticut, a rental car company ticketed a customer for speeding in its rental car. The way the company knew the customer had unlawfully sped was thanks to a global positioning system (GPS) installed in the trunk of the car. The customer sued the rental company since he felt he had not been properly notified of the GPS device. Not only is the use of new GPS technology a concern, but so is the fact the rental car company in effect became a policing force. Until now, penalizing drivers for speeding has been a police function.

Dataveillance increases social monitoring, resulting in heightened social control by more parties. Enforcing lawful behavior is now a government *and* a business venture. Today there are a number of examples in which the lines between commercial and government interests blur and the public and private sectors work together in joint dataveillance endeavors.

A friend of mine discovered this last summer in a somewhat costly manner. He moved from upstate New York to New York City and decided not to inform his car insurance company of his move immediately, knowing his insurance costs would increase significantly. After moving to New York City, he bought

an E-ZPass card to speed up his commute to work. The E-ZPass system is run by an organization comprised of five state transportation agencies. It functions as an automatic electronic payment plan allowing drivers to keep moving as they pass through toll stations.

Soon after purchasing the E-ZPass card, my friend got a letter in the mail from his insurance company notifying him that his rates had doubled due to his relocation. Upon calling the insurance company, my friend found out the company knew of his move thanks to the E-ZPass database. The two organizations were sharing information for each other's benefit. My friend was unable to afford the new insurance policy and, thus, forced to give up his car. The joint efforts of a state organization and a commercial insurance company produced compliance and lawful behavior.

My examples so far have been about data-collecting practices in which an individual is identifiable and there are personal consequences. But David Lyon specifically states that dataveillance is "the collection and processing of personal data, *whether identifiable or not*…"(Lyon, Surveillance Society 4). How then can anonymous data-collection contribute to the "managing [of] those whose data has been garnered" if names are withheld? How does social ordering function without individuals?

The type of social ordering that deals in anonymous data is knowledge production used to influence populations on a more general level. Lyon writes: “Surveillance today is a means of sorting and classifying populations and not just of invading personal space or violating privacy of individuals…. Surveillance has become an indirect but potent means of affecting life chances and social desires” (Lyon, Surveillance Society 151).

This happens on a daily basis in the most banal ways. Why does a chain store open in a certain neighborhood and not another? Why are certain coupons available at one supermarket and not the same supermarket five miles down the road? These decisions are based on generalized data bits: census data, zip codes, probable incomes, market trends and the like. Some of this data is available for free (i.e., census data), some of it retail companies collect on their own (i.e., customer zip codes, product movement) and some is processed and analyzed by third companies whose business is information management. Companies covet this type of data, as a means to reduce business risk and ensure a healthy, successful marketplace.

One result of commercial reliance on anonymous data is the speeding up of standardization in the marketplace and the disappearance of anything marginal. On a recent visit to a bookstore with my mother, we could not find an art magazine usually on the shelf. My mother shared her dismay with the shopkeeper and his response was that those types of magazines did not

"move fast enough" and were therefore phased out. It struck me at the time that this is what is happening across the country on an accelerated scale thanks to database culture. What is "popular" or what sells is reinforced while what is not "hot" is quickly dropped from inventory. Choice in the marketplace is close to non-existent, and allegiance to market data propels this reductionism. Businesses boast they are giving the public what it wants, but if desires are being produced and met in a continuous data feedback loop, who can really say?

Non-identifiable data is used for a variety of other purposes, some having more serious repercussions than dissolving market diversity. For instance, CBS News reported on March 19, 2002, that airports are using census data to locate passengers from high-crime neighborhoods who may face extra screening (CBS News). Lyon critiques another practice: health insurance companies denying individuals coverage or increasing premiums due to demographic data. He states that "the risk management approach…is based on a profoundly utilitarian moral calculus that effectively displaces other moral criteria such as generosity, guilt or fairness" (Lyon, Surveillance Society 10). He later elaborates with a vivid analogy:

> [Surveillance] undoubtedly has the effect of reinforcing social differences and divisions. An analogy with New York planner Robert Moses' very physical and visible low bridges and underpasses helps here. Moses created height restrictions that prevented buses carrying black and poor people from reaching certain quarters of the city. I argue that new technology surveillance systems continue this invisibly

> today, affecting life chances through categorization and risk management (25).

Foucault, Mark Poster and the Superpanopticon

The work of Michel Foucault is pertinent to this idea of social control through data categorization. A thorough analysis of Foucault, or any other theorist for that matter, is outside the scope of this paper, but I will explore a few intersections between modern-day surveillance systems already described and critical theories of social ordering, subjectivity and database language.

Although Foucault never discussed digital technologies, he is responsible for focusing attention in critical circles on the issue of surveillance and, in his words, technologies of power. Foucault would never have called his writings a "theory" of power since to do so would suggest universal meaning (static theory) of a thing (power); he also denied that he was an analyst of phenomena termed power. Instead his objective was "to create a history of the different modes by which, in our culture, human beings are *made* subjects" (Dreyfus and Rabinow 208). The general theme of his work, therefore, was not surveillance or power, but subjectivity. He spent much time discussing issues of power since for him the making of a subject has much to do with power relations. Power for Foucault was a means to discuss his prime interest, "studying the objectivizing of the subject" (Dreyfus and Rabinow 209).

Objectification of the subject has developed with modern day science and can be seen on a parallel course with the move toward rationalization in the West. But for Foucault, rationalization should not be seen as an all-encompassing progression, instead as multiple rationalities. This distinction led him to study specific fundamental experiences (i.e., madness, crime, sexuality) that society seeks to eradicate through scientific method. Foucault's purpose was not to critique an institution or group (i.e., insane asylum, prison, bourgeoisie), but rather technologies of power. The technologies of power are the disciplinary tools or practices used to correct deviance. Technologies of power do not operate through repression of desire (as in Freudian theory), but through classification, tabulating and organizing desire (Lyon, The Electronic Eye 209).

Power, irreducible to an institution or exterior force, must be considered at the micro level of experience. Power relations, according to Foucault, are rooted in a system of social networks (Dreyfus and Rabinow 224). By mistaking power as a thing working outside and independent of us, power becomes an autonomous force—and therefore unyielding. Hubert Dreyfus and Paul Rabinow claim:

> For Foucault, unless these unequal relations of power are traced down to their actual material functioning, they escape our analysis and continue to operate with unquestioned autonomy, maintaining the

> illusion that power is only applied by those at the top to those at the bottom (Dreyfus and Rabinow 186).

Foucault aims to illustrate how local actions performed intentionally by a subject feed into larger systems of power that are not necessarily coordinated. In Foucault's words, "People know what they do; they frequently know why they do what they do; but what they don't know is what they do does" (Dreyfus and Rabinow 186).

The man who manufactures and sells magnetic strip scanners knows what he does (sells card scanners) and why he does it (to help companies quicken authorization processes and subsequently acquire cheap databases). He is, however, probably unaware of the broader consequences, the social implications, of his actions. What he does is inaccessible to him. Conversely, people who hand over their licenses to be scanned knowingly and do not care that their personal information is collected and utilized are equally unaware. They are trapped in the notion of individuation: I can handle the world knowing that I bought a pack of cigarettes today in this place and at this time. They do not follow the trace of their actions into the realm of power relations. Foucault draws connections between micro, everyday actions and macro social relations attacking the perception of power as an exterior, autonomous force.

Foucault's most famous example of a disciplinary technology in operation is, of course, the Panopticon. In Discipline and Punish: The Birth of the Prison, Foucault explains Jeremy Bentham's plan for the Panopticon (1791) like this:

> [A]t the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other,on the the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower…the small captive shadows in the cells of the periphery. They are alone, perfectly individualized and constantly visible. The panoptic mechanism arranges spatial unities that make it possible to see constantly and to recognize immediately….Visibility is a trap….He is seen, but he does not see; he is the object of information, never a subject in communication (Foucault 200).

The Panopticon is an efficient, continuous, flexible, and comprehensive piece of architecture for administering discipline. Efficient because it depends only on light and positioning. Continuous because the observed are unaware of when the watchtower is occupied and, therefore, must behave as if surveillance is constant. Flexible because the plan is multi-purpose (works in a prison, hospital or workplace) and anyone can fill the role of the observer or the observed. Comprehensive because not only is the observed regulated,

monitored and controlled through observation, but so is the observer. Activity in the central tower manipulates the behavior of everyone involved.

It does not take much imagination to carry this example a step further into today's world of dataveillance. The very structure of panoptic surveillance mirrors the invisible and constant flow of dataveillance. Everyone is implicated in its network. Anyone can carry out the different roles of observer versus observed and can even find themselves simultaneously in both positions. Foucault's description of the subject inside the Panopticon ("he is the object of information, never a subject in communication") is a beautiful summation of database language. It is a one-way communication channel. You are entered into the system and there you remain observable, malleable and without voice. In Mark Poster's words:

> In [the case of the database] the individual is not addressed at all; he or she receives no messages. Rather the communication goes the other way round. The individual, usually indirectly, sends messages to the database. In one sense the database is nothing more than a repository of messages (Poster, The Mode of Information 69).

Mark Poster has updated Foucault for the 21st Century. For him, the database is the newest structure of domination (or in Foucauldian terminology, technology of power). He considers the database a major force that constitutes subjectivity today. The database does this through manipulating relationships between bits of information. These relationships do not exist outside the database and only begin inside its system.

Poster calls the discourse of the database the Superpanopticon. He ties his database analysis to Foucault's Panopticon in this way:

> Foucault taught us to read a new form of power by deciphering discourse/practice formations instead of intentions of a subject…. Such a discourse analysis when applied to the mode of information yields the uncomfortable discovery that the population participates in its own self-constitution as subjects of the normalizing gaze of the Superpanopticon. [In this way] databases [are] not…an invasion of privacy…a threat to a centered individual, but [a] multiplication of the individual, the constitution of an additional self, one that may be act upon to detriment of the "real" self without the "real" self ever being aware of what is happening (Poster, The Mode of Information 96-97).

The data-self is therefore both created and regulated within the database. Due to the "objective" nature of its language (numbers, abbreviations, acronyms, codes) and its scientific appearance, the data-self carries a certain cache and authority that acts upon the physical self and eventually becomes more trusted than the physical self. In this way, the database becomes a discursive, organizational practice and an essential technique of power in today's social field.

Heiddegger and Understanding the Data-Self as Being-in-the-World

Martin Heidegger is probably not the most obvious philosopher to reference when discussing the data-self and dataveillance. However, I feel there are

some ways in which his ontological preoccupations and his investigations into Being-in-the-world are relevant as well as revealing.

Heidegger's ontological study in Being and Time starts with the question concerning the meaning of Being and those who ask the question in the first place (Dasein). Dasein, as the primary entity for his analysis, cannot be reduced to a subject, soul, consciousness, spirit or person. Rather, Dasein is somehow subject and object, investigator and that which is investigated, always already accessible and that which we want to access.

Immediately in Being and Time, Heidegger questions the traditional philosophical pursuit of knowledge (object) via a separate and disinterested individual (subject). For Heidegger, consciousness or reflective, mental activity is a secondary function derived from a more basic state of Dasein's Being-in-the-world.

Being-in-the-world is a fundamental structure of Daesin. Heidegger states:

> In the interpretation of Dasein, this structure is something 'a priori'; it is not pieced together, but is primordially and constantly a whole. It affords us, however, various ways of looking at items which are constitutive for it. The whole of this structure always comes first… (Heidegger 41).

As a fundamental structure, Being-in-the-world—which can be summarized as Dasein's ongoing, everyday activity of absorption into the

world—determines the character of Dasein and is therefore essential to understanding Dasein. Being-in-the-world is a non-thematic, non-reflective activity of average everydayness. For Heidegger, Being-in-the-world preceeds any notion of understanding the world. Understanding cannot be thought of as something we direct ourselves with purpose towards, but rather we project ourselves into it constantly.

Heidegger discusses our relationship with a hammer as an example of this kind of understanding. When we use the hammer (or any other piece of equipment), our concern for it as an object is subordinate to our act of using it. We seize hold of it, use it and—if everything goes smoothly—we set the hammer aside and move on to something else. This kind of activity, activity that is not contemplated during the act of doing or even premeditated, is basic to our everyday dealings in the world. The hammer is, in Heidegger's terms, ready-to-hand or available to us. It is knowable through our use of it without mental reflection.

The hammer, in this case, is a lived meaning rather than a concept. A hammer, of course, can become a concept or become present-to-hand rather than ready-to-hand. This transition, in which equipment distinguishes itself and becomes apparent, happens when things go wrong. If the hammer is too heavy, if the hammer snaps in half, suddenly the equipment is "there" before

us and made obvious as some thing rather than a part of action situated in the world.

This moment of breakdown is not how we usually behave, but it is not negative. It is, in fact, an important shift out of habitual routine. At this moment, Heidegger writes “the context of equipment is lit up, not as something never seen before, but as a totality….With this totality…the world announces itself” (74-75). The moment involvement stops, understanding does not stop but potentially proceeds towards a new status of Being, interpretation. A network of possibilities opens up and if we choose to work through them, interpretation gives way to meaning. Meaning, therefore, is not an exterior value stuck onto some thing, but is discovered alongside or along with the meaning of Being.

How, then, does this relate to the data-self? In what ways does Heidegger’s abstract, philosophical doctrine become useful to our lives in the 21st Century? I believe it is helpful to approach the notion of the data-self in a Heideggerian fashion; the data-self is not a separate thing detached from our being in the world, but rather an integrated part of ourselves that is indistinguishable from and intertwined with our being. In a dataveillance world, we are born along with our data-selves. When we take our first breaths in the hospital, our data selves are already present and developing with us. Today, 226 data bits are produced on average by the time an infant is

released from the hospital (Doyle, Lane, Theeuwes, and Zayatz). Currently, there is not a moment when we live without our data-self.

This data-self, however, is not noticeable or even acknowledged on a regular basis. This is one reason why issues of dataveillance are so hard to raise. Without explicit understanding, there is no concern. Explicit understanding, however, does happen from time to time. The example of my friend buying an E-ZPass is one such time. The moment he realized the connection between his insurance price hike and his purchase of a commuter card, the network of operations became clear. This is similar to Heiddeger's example of the hammer breaking; when there is failure, involvement stops and suddenly a totality of interconnections comes into focus. For my friend, due to his failure to comply with the law, there was a sort of breakdown. The system acted in order to fix the unlawful behavior and enforce compliance. Through this disruption from everyday life, my friend was able to understand the network more fully. Hence, his data-self became an object outside himself that he could contemplate and consider.

This is the first step towards resistance. Understanding and interpretation by individuals is necessary groundwork for resistance. Unfortunately, as previously mentioned, these moments of breakdown are rare because dataveillance effectively produces compliance through its invisibility, technical language, promoted benefits and speed. Today, however, there are some

individuals and groups who actively produce spaces for this kind of understanding and interpretation as a means to encourage social resistance to dataveillance. Art is an important field in which this is happening.

Part Two: Data Poesis and Resisting Dataveillance through Art Practice

Introduction

I am personally interested in and involved with net.art as a form for data resistance. There are other artists and art collectives critiquing data collection practices and methodologies vary. Most aim to educate the public or force systematic breakdown or a combination of the two. Thus far, my own work has been primarily educational. I will discuss two of my recent projects, “Self-Portrait version 2.0” and “Online Private Investigation (O.P.I.): The Bill Joy Project” and works by others that have in some way influenced me or have similar goals as mine. Common to all the works I will discuss is the general desire to reclaim data from the control of the few. Or, to use Steve Dietz’s term, the common goal is datapoesis, the “freeing of data for a different trajectory” (Dietz, par. 12). A new media curator, Dietz coined this term in his article “Memory_Archive_Database v 3.0” to describe a growing trend in art toward destabilizing classification activities. The Internet is a fine space to practice datapoesis not only because it consists of data bits, but also because

it is accessible to a general public and its very structure is flexible allowing for the blurring of strict divisions.

Rachel Schreiber comments on this last point in her essay “Net.art: Shedding the Utopian Moment?” She acknowledges the truly subversive nature of net.art since it is completely indistinguishable from its commercial counterparts (Schreiber 52). Because net.artists use the exact same tools and means of production as commercial web builders, net.artists can fool a viewer into believing a site is “real” when in fact it is a corporate parody that aims to undermine corporate language and positioning. Freeing data for a new trajectory becomes more possible in spaces where strict boundaries can be temporarily suspended and manipulated by a general public.

While my projects are mainly Internet specific, there are other art projects dealing in datapoesis that exist offline and are not at all Internet related. There are also projects addressing datapoesis that successfully tackle both cyber and embodied world experiences. These, perhaps, are the strongest works because they move fluidly between realms showing how interconnected cyber cultures are with our lived, world experiences. I will share examples of all three kinds of projects.

Self-Portrait version 2.0

My first “datapoesis” project was “Self-Portrait version 2.0” (SPv2), an online application available at http://www.spv2.net completed in late 2001. SPv2 explores how identity can be constructed and perceived through data collection in cyberspace. Some data in cyberspace we consciously create to represent ourselves (emails and web sites, for instance). Other bits of data accumulate without our efforts—and many times without our knowledge—tracing certain of our interactions both in the physical and virtual worlds. Because of this data we do not willingly disperse, our cyber image is not always in our control nor ever fully knowable to us. SPv2 explores to what extent we are accessible online and what we may look like through mining Internet data (see fig. 2).

When you enter SPv2, you can choose to activate data from three categories: *DataMine, DataWake and Join Me!. DataMine* includes that data I actively create or view in my everyday life: my incoming email, my local weather and my personal web cam. *DataWake* is the data that accumulates as a byproduct of my interactions in the physical and virtual words. This includes web search results from my name, my clickstream data (or my web surfing data), my consumer profile, my voter registration information and my FBI file. As the users make their selections, SPv2 grabs data from the chosen source, translates the data into a visual representation and displays it to the user.

One may layer the various visual depictions to eventually achieve data chaos.

In the third section, *JoinMe!*, a user is asked to enter her/his name and zip code. With this input, SPv2 searches the Internet and dynamically collects data about the user to incorporate into the portrait. After the user's "image" is displayed, the user is rewarded for participation with access to recent *JoinMe!* logs. The person is rewarded, but also realizes that their information will be viewable to the next person. Therefore, users are not only voyeurs, but are objects for inspection. Participation usually makes one see or feel the benefits, but hardly ever the consequences.

SPv2 updates the genre of portraiture for the information age. In the history of Western art, portraiture traditionally fulfilled the purpose of reinforcing wealth and power. SPv2 is an inversion of this power structure; it results in a reconstruction of the self after it has been digitized, analyzed, shared and sold.

In a review of SPv2 appearing in the art journal "AfterImage," Ricardo Miranda notes:

> The fact that Singer has chosen to reveal these files, particularly the self generated files such as the Webcam and Email, points to the delight of many Internet participants who choose to reveal their private life to a vast anonymous audience. The concept that many people enjoy the attention of a public stage and make use of the Internet for that purpose is not new. But the juxtaposition of DataMine and

> DataWake makes explicit the complexity of the Internet as a sphere that we help compose for our enjoyment, though it may have regulating and normalizing effects (Miranda 8).

This comment alludes to the experiences in everyday life—off or online—in which the private and public converge and further call into question the already tenuous boundary between the two. Where voyeurism meets surveillance is a slippery slope that I have experienced in my own online investigations. Often times the softer language of voyeurism candy-coats or reduces the iron grip of surveillance, allowing a person to proceed with less difficulty. There are no ethical dilemmas for me when I use myself as subject, as in SPv2. My subsequent project, however, leaves the safety zone of self-objectification as I venture into investigating other people's data-selves. The results are attention getting but lead me to ask questions. How far can I exploit the dataveillance system in order to gain attention and start a critical dialogue about its existence and use? Where must I personally draw the line? Is targeting an individual, even if he or she "deserves" it, taking the experiment too far? These questions are for now rhetorical as I continue to consider them through my art-making process.

Online Private Investigation (O.P.I): The Bill Joy Project

"Online Private Investigation" (O.P.I.) came directly out of my research and production of SPv2. O.P.I. began with an online investigation into an

individual, Bill Joy. I gathered considerable information, including but not limited to a background search, real estate holdings, voter-registration information, the individual's company profile, salary information, pending patent information, driver's license information, a marriage license, company emails and census data. I allowed a select group of people to review the resulting dossier (see fig. 3). This group was a mix of people of all ages and backgrounds. I was also interested in creating a group of different disciplines. In my group, there was a Jungian psychoanalyst, a lawyer, an architect, a business consultant, a video artist, a physical therapist, a university student and others.

After my participants thoroughly read the dossier, they wrote a brief description of Bill Joy. Next they took a Myers-Briggs personality test and answered several short questions from the perspective of Bill Joy. The questions were taken from the back page of "Vanity Fair" magazines. The back page is devoted to what is called the "Proust Questionnaire" in which celebrities answer questions like: "Which living person do you most admire?" and "If you were to die and come back as a thing, what thing would you be?"

I used the responses to paint a collective portrait of this person (or the person perceived via the data file). The particulars of the file were not part of the final piece. Rather, the focus became the persona that emerged from the various readings of the dossier. Also, no one participant was quoted or credited. Instead, I wove the responses together to create a multi-faceted, and perhaps

conflicting, picture of an individual realized through data. The result of this process (as of now) is a series of posters that are “O.P.I Made for Bill Joy” (see fig. 4-5).

So why Bill? Bill Joy is one of the co-founders of the technology company Sun Microsystems. At Sun, he promotes the abandonment of the personal computer in exchange for a low-tech device that runs off powerful corporate-controlled servers. What this means is the network you are connected to, not the box on your desk, will do the job you want done. The appeal is that consumers will not have to handle so many technical problems, but the major danger is centralized control of personal computing. Sun has repeatedly declared that the reign of the PC is over. Networking is king. In addition, the CEO at Sun, Scott McNealy, is (in)famous for his statement, “Privacy is dead. Get over it.”

The coupling of centralized supercomputing with a disregard for privacy is a scary thought. The ability to collect, store and access large amounts of information on individuals would be even easier than it is today. In addition, the capacity for analyzing this data for the purpose of predicting and controlling behavior would increase dramatically.

Bill Joy was just a proxy. Most of the information in his data dossier comes from public records that are maintained in the United States, records increasingly found online. These records exist for all U.S. citizens.

This project is unfinished and will take other forms before it is completed. In this first instance of O.P.I., my participants were my main audience since they were privy to the complete data file as well as the resulting posters. For ethical, reasons I withheld the details of the file from a larger audience, but informed them of its existence. The instructional dimension of the project (what kind of personal information is accessible online, where does one get it and what does it look like) is therefore reserved for my participants. What becomes apparent to a larger audience that views only the posters is the realization that this *kind* of online investigation can be done and is done. Furthermore, the posters underscore the subjective function of reading a data dossier. My attempt to design an object for a person via his/her data-self brings what normally is considered scientific into the realm of subjective art making. As I cross the boundary between art and science, I am calling into question both disciplines and asking my viewers to consider art via science and vis a versa. I am freeing data for a new trajectory: to educate people about personal data available online and encourage its more careful consideration.

Other Projects

Mark Lombardi was an artist who was fascinated by the flows of data, both the abstract patterns the flows create and the very concrete—yet often strange—relationships that develop in its path. Lombardi's drawings record political influence (in solid lines) and financial transactions (in dotted lines). His drawings impress the viewer with their sheer amounts of information and the complex schemes that emerge. They expose strange bedfellows like George W. Bush and Osama Bin Laden in a prescient 1999 drawing describing energy-related business ventures (see fig. 6). The drawings shimmer like celestial maps "because of lines and arcs connecting circles which carry the names of institutions and individual players" (Moshkovits, par.2).

Lombardi studied reams of news reports and financial records to create his drawings that seem to "set the record straight." Whether his analysis of events and their interconnectedness is the "truth" or not is really beside the point. As the title of his first solo show, "Silent Partners," suggests, Lombardi was most interested in "outing" an elite group of people whose secret actions and transactions have had—in one way or another—an immense impact on the world. He translated hard-to-find and hard-to-read documents into fascinating galaxies opening up the material for a wider audience to view and interpret via his own processing. He made data concerning busted banks, hot

money and financial fraud into sweeping structures sometimes as large as 10-feet wide and invited viewers to enter, engage and, of course, question.

“They Rule” by Josh On and Futurefarmers is an interactive web site that is similarly preoccupied with mapping power relations and exposing information. At Theyrule.net, a person can choose from a long list of U.S. companies and see, among other things, the specific board members who run the company. By clicking on other companies, the relationships between the corporations and their board members are graphically displayed and soon the immense amount of capital that is concentrated and controlled by few individuals becomes clear.

Elegantly computer-drawn maps and icons stimulate the viewer of “They Rule” in a manner similar to Lombardi’s drawings, but with a major difference: in “They Rule,” the viewer is actively revealing the bits of information and takes part in discovering connections between people in power. While Lombardi did not use the Internet for his art (although perhaps for his research), Josh On and Futurefarmers’ final product is all about the web. “They Rule” utilizes the vast resources of the web by linking its data bits to other, outside web sites that offer more information and the possibility for further research by viewers. The network of meaning is ever-expanding through the web. Also “They Rule” has utilized the viral quality of the web for broad dissemination. The effects of the two projects are simpatico, however.

They both expose power relations through data that is too often “hidden in plain sight.”

“iSee” by the Institute for Applied Autonomy (IAA) is also an interactive web site and confronts the issue of surveillance, specifically the issue of surveillance cameras in the United States. Using maps of surveillance camera locations in New York City created by the Surveillance Camera Players, “iSee” generates interactive maps that will help a user find a route with the least amount of resistance (or the least number of surveillance cameras) in downtown Manhattan. A user clicks on a starting point and then clicks on a destination point and “iSee” will suggest a route that dodges the most number of camera locations. It may not be the fastest path, but it is the path with the least number of electronic eyes.

As of now, the project is more a gesture towards resistance since it is limited to the somewhat outdated information provided by the Surveillance Camera Players and to New York City. IAA, however, has plans to expand to other cities and to make its system compatible with wireless mobile devices (cell phones, PDAs, pagers) allowing users to update the camera location database dynamically and to utilize the map-maker in the field (or on the city street). This next version of “iSee” will seamlessly integrate the knowledge resource of the IAA database and the “iSee” community in a way that will enable more effective resistance while empowering its community of users.

And lastly, Mark Daggett has produced a variety of net.art sites that on the surface appear colorful and entertaining, but on deeper consideration are more scary than fun. As Alex Galloway of Rhizome.org said, "Mark is rapidly becoming the artist whose work you're afraid to look at" (Mirapaul, par.6). Daggett's most recent project is titled "VCard." The cheery pink hues and the welcoming heart on the home page make one think the site is all about sending electronic Valentines. Yet it becomes clear as you read the fine print that the "V" is not necessarily for Valentine. The "V" more likely signifies an equally infectious—but less pleasant—thing called a virus.

"VCard" is in fact an artist-made virus. At the "VCard" web site, a user can enter a person's email address and a personal message. The message will be sent along with an attachment. The attachment consists of three images randomly picked from the sender's hard drive. If the recipient opens the attachment, the images will flicker in succession with the message, but that is not all. By opening the attachment and agreeing to the "VCard" terms, the recipient has in effect agreed to send three images from his/her hard drive to every person in his/her email address book. The cycle continues as long as recipients open the attachments and agree to the "VCard" terms.

Since there is notification of intent in the "VCard" terms, this is a polite and gentle virus. Nonetheless, "VCard" does point toward the risks of online

privacy and suggests the uncontrollable power of code to non-techies. "VCards" is similar to an earlier project by Daggett called "Deskswap" in which a program takes snapshots of users' computer screens and sends them through a network for others to view. "Deskswap" is billed as a collaborative screensaver program, but what you are contributing is the ability for unknown entities to view your desktop. A desktop can, of course, be a very boring affair, but it can at times contain personal information beyond what an average person may wish to openly display.

Daggett's projects are less instructional than hype. They play on people's fears concerning online privacy and fail to offer tools to foster resistance or even understanding. Rather, Daggett is using techniques already widely popularized to fuel the mystery surrounding online privacy, meanwhile making users' feel even more victimized. His projects hi-light the "gee-whiz" aspect of tricky code, but do nothing to alleviate common misperceptions about dataveillance.

Conclusion

There has been a developing movement, especially in the past ten years, of artists utilizing data as a medium or as content matter. This work addresses broad issues, such as who has access to what information and how it is read or organized to produce meaning. Newer trends include technological

situations led by artists to inform the public of surveillance techniques and to propel systematic breakdown. The most successful of these projects provide spaces for understanding and interpretation by viewers through temporary breakdown of dataveillance systems.

This type of practice is an important complement to the activities generated by privacy advocates. The two fields are not always distinguishable nor should they attempt to be. However, the art practice is well suited for educating audiences while simultaneously opening up issues for consideration and discussion. Such discussions can successfully blend the languages of art, politics, economics, philosophy, and social theory. Furthermore, since art forms can be fluid and art boundaries are contestable, artists are able to counter the invisible grip of dataveillance in ways meaningful to society.

Works Cited

American Civil Liberties Union. “Do you know where your data is?” May 14 2002.<http://www.aclu.org/action/privcard.html>

Camera Surveillance Players. “SCOWTing out surveillance cameras in Manhattan.” Nov. 37 2001. May 14 2002. <http://www.notbored.org/scowt's-honor.html>

CBS News. “An Airport Security Secret.” CBS Evening News. March 19 2002 Transcript. May 14 2002. <http://www.cbsnews.com/stories/2002/03/19/eveningnews/main504093.shtml>

Dietz, Steve. “Memory_Archive_Database v 3.0.” Switch Journal. January 21 2000.<http://switch.sjsu.edu/nextswitch/switch_engine/front/front.php?artc=31>

Dreyfus, Hubert and Paul Rabinow. Michel Foucault: Beyond Structuralism and Hermeneutics. Chicago: University of Chicago Press, 1982.

Doyle, P., J. Lane, J. Theeuwes, and L. Zayatz, eds. Information Explosion. “Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies.” Washington, DC: Urban Institute, 2001.

Electronic Privacy Information Center. “Public Opinion on Privacy.” May 14 2002. <http://www.epic.org/privacy/survey/>

Federal Trade Commission. “FTC Recommends Congressional Action to Protect Consumer Privacy Online” May 22 2000. May 14 2002. <http://www.ftc.gov/opa/2000/05/privacy2k.htm>

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

Goldhamer, Don. “The Right to Privacy: the Law and the Constitution.” May 14 2002. < http://home.uchicago.edu/~dhgo/privacy-intro/dsld07.html>

Heidegger, Martin. Being and Time. New York: Harper & Row, 1962.

Hibbert, Chris. “Frequently Asked Questions on SSNs and Privacy.” Computer Professionals for Social Responsibility. Feb 16 2002. May 14 2002. <http://www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html>

Junkbusters. “Yahoo weakens privacy policy.” May 14 2002. <http://www.junkbusters.com/new.html#YHOO >

Lee, Jennifer. “Welcome to the Database Lounge.” New York Times 20 March 2002, Circuits Section. May 14 2002. <http://query.nytimes.com/search/abstract?res=F70714FF3B5C0C728EDDAA0894DA404482>

Lyon, David. Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press, 2001.

– – –. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 1994.

Miranda, Ricardo. “The Work of Artists in a Databased Society: net.art as on-line activism.” Afterimage: The Journal of Media Arts and Cultural Criticism. Vol. 29, No.5, March/April 2002: 7-9.

Mirapaul, Matthew. “A Greeting Steals Its Way Onto Your Hard Drive.” New York Times 11 April 2002, Circuits Section. May 14 2002. <http://query.nytimes.com/search/abstract?res=F2091EFB35590C728DDDAD0894DA404482>

Moshkovits, Boris. “Mark Lombardi: Pierogi2000.” Flash Art. May 1999. May 14 2002. <http://www.pierogi2000.com/press/lombardi.html>

Poster, Mark. The Information Subject. Amsterdam: G & B Arts International, 2001.

– – –. The Mode of Information. Chicago: University of Chicago Press, 1990.

Pew Internet & American Life. “Trust and Privacy Online:*Why Americans Want to Rewrite the Rules.*” Aug. 20 2000. Pew Research Center for People and the Press. May 14 2002. <http://www.pewinternet.org/reports/reports.asp?Report=19&Section=ReportLevel1&Field=Level1ID&ID=43>

Privacy Journal. May 14 2002. <http://www.townonline.com/privacyjournal/>

Privacilla. “Privacilla’s Two Part Definition of Privcay.” May 14 2002. <http://www.privacilla.org/fundamentals/privacydefinintion.html>

Privacy Foundation. Interview with Richard Ellis Smith. “Catching Up with the "Ralph Nader of Privacy." May 14 2002. <http://www.privacyfoundation.org/resources/intRESmith.asp?id=40&action=0#guide>

Rosen, Jeffery. “Silicon Valley’s Spy Game.” New York Times Magazine 14 April 2002: 46 –51.

Schreiber, Rachel. “Net.Art: Shedding the Utopian Moment?” Link: A Critical Journal on the Arts in Baltimore and the World. Issue 7, Fall 2002: 48-57.

Tech Law Journal. “DoubleClick Changes Data Collection Plans.” March 6 2000. May 14 2002. <http://www.techlawjournal.com/privacy/20000306.htm>

Warren, Samuel D. and Louis D. Brandeis. “The Right To Privacy.” 4 Harvard Law Review 193, 1890.