Surveillance Creep! New Manifestations of Data Surveillance at the Beginning of the Twenty-First Century

Preemptive Media (Beatriz da Costa, Jamie Schulte, and Brooke Singer)

A young woman goes to a liquor store to buy a bottle of wine. At the checkout counter, she is asked to present her driver's license—the usual procedure in the United States for any person who looks under thirty. The woman hands over her license to the clerk, but what happens next surprises her. On this day, it is not business as usual. Instead of looking for her date of birth, the clerk swipes the driver's license through a small machine under the cash register. The young woman does a double take; had she handed over her credit card by mistake? When she takes her card back, she studies it closely. Yes, indeed, it is her driver's license, but for the first time she notices a magnetic stripe on its back side, one very similar to that of her credit card.

A number of thoughts run through her mind. Why did the clerk not simply look at the face on the license to ensure she was of age? What information is on that stripe besides her date of birth? Is it only being read, or did the clerk copy the encoded information? And if her information were saved, what would the store do with it anyway?

A story much like this one inspired the authors of this essay to take a closer look at driver's license card technologies and the industry family to which they

Radical History Review
Issue 95 (Spring 2006): 70–88

belong: Automatic Identification and Data Capture (AIDC). The purpose for using magnetic stripe technology, and for AIDC technologies in general, is to identify people or objects through machine-automated processes. These kinds of technologies are on the rise and cropping up in the most routine tasks of our everyday lives. How has this come about, and what is the motivation behind the current trend toward the implementation of AIDC on a massive scale?

In the story above, for example, the owner of the liquor store might argue that machine-automated reading of a magnetic strip makes the sales clerk's job easier and, therefore, more efficient. The clerk does not have to worry about making others wait in line as he or she tallies up the customer's age; a machine does it much more quickly. The store might also claim that a magnetic stripe is much harder to tamper with than the face of the driver's license, therefore making fraudulent IDs easier to detect.[1] Both efficiency and fraud prevention ultimately save the business money, since a liquor store not only wants to serve customers as quickly as possible but also wants to avoid costly lawsuits that result from selling alcohol to minors.

After a little independent investigation into the matter, however, it became clear to us that this technology is used primarily for less publicized reasons. As the verification of ID is how AIDC is advertised to the public, this is what the store tells its customers and why the machine's screen openly displays a person's age after a valid ID is swiped. But the hidden benefits—what goes on out of sight—are data collection, data matching, and data analysis. The president of Intellilink, a manufacturer of ID verification systems, states in an industry article that "not only are the retailers [who use our system] complying with the law by carding, but at the same time they have compliance, they're also building a database of information."[2] Such a database, nearly free of charge and one that neatly collects information to build a customer base, is arguably the most important benefit a card-verification system brings to a business and, in some cases, to the U.S. government as well.

This essay explores current and proposed uses for AIDC technologies, focusing primarily on the already widespread practice of driver's license swiping in the United States. Driver's license swiping exemplifies several of our greatest concerns related to AIDC: the invisible or discreet nature of most AIDC technologies; the lack of notification and consent by subjects; the largely unregulated and unaccountable data collection and usage practices by U.S. businesses; the interdependence of business and government interests; and the encouragement of what some might call surveillance creep into every facet of contemporary life. It is our belief that a critical assessment of and informed reaction to AIDC must not be reserved exclusively for an expert community because the continued use of AIDC technologies has the potential to transform almost every aspect of our everyday lives. However, in order to enable the public an opportunity to debate its development, deployment, and regulation, a certain amount of background understanding is required.

The AIDC Industry and Technologies: A Technical Overview

Automatic Identification and Data Capture (AIDC) is a family of technologies for the unique identification of physical objects by automated processes. These technologies are designed to bridge the gap between entities in the real world and computer databases that describe them. AIDC endows a computer system with a set of eyes that can uniquely identify any object that is appropriately tagged. Computer algorithms designed to improve efficiency can then work with direct and immediate knowledge of the environment, rather than process statistical information collected by hand at a prior date.

Applications of AIDC have been around for decades, and they now include retail checkout, warehouse inventory, livestock management, vehicle driver's licenses, and keyless building entry systems. The AIDC industry profits by creating new systems that reduce the human effort required to perform tasks relating to recognizing objects. AIDC takes the human out of the loop and thus reduces labor costs, accelerates the movement of products, and, in theory, reduces the potential for error, fraud, and sabotage. In addition, by facilitating data collection, AIDC allows for the accumulation of large volumes of information.

On one hand, AIDC addresses an old technological problem: how can a computer identify an object in the real world? As of 2005, computer vision research has not yet come close to producing systems that can visually recognize objects in a natural environment without significant error. Even if vision worked well, a computer would be unable to distinguish between different objects that have the same appearance. To reduce this problem, AIDC focuses on techniques that involve tagging objects with data encoding that can be interpreted more directly by the computer. The earliest and most obvious example of object tagging is the bar code, which is printed on the package of virtually every product sold by large retailers in modern industrial economies. More recent innovations, such as magnetic stripe cards and so-called contact smart cards, are typically used to identify consumers rather than products. Currently in development are radio frequency identification (RFID) technologies, which have shown promise as an advanced method of identifying both products and people with minimum labor.

Since their standardization in the 1970s, bar codes have accelerated the flow of products in commercial and industrial settings. Bar codes come in different sizes and encodings. The simplest variety is capable of representing short numbers only, whereas later designs can encode a short paragraph of text from the ASCII character set. In the United States, a product such as a tube of toothpaste is marked with a simple bar code that encodes the numerical Universal Product Code (UPC). In most of the rest of the world, the European Article Number (EAN) system is used. During checkout, the UPC symbol simply indicates the brand and type of product that has been scanned, while the retailer's database links this to the product price, the number remaining in inventory, and (in some cases) the purchasing history of the

individual consumer. In retail environments, bar code systems are inexpensive to implement because most products are already marked with a UPC symbol, but they require careful scanning by a human operator. More advanced encoding schemes, often called two-dimensional bar codes, consist of a square region filled with small black-and-white pixels and can represent a greater quantity of information. Two-dimensional bar codes are used on some ID cards and by the U.S. military and have been adopted in China as the national standard for bar coding.

The unique identification of people as opposed to commodities by machines presents a different set of challenges. Even though bar code tattoos indeed exist, they are generally not embraced by the mainstream, and many people will circumvent identification systems when technologically possible. However, involuntary subjects such as prisoners, animals, and students have been marked with radio badges, ankle bands, or injected subdermal RFID chips. For everyday ID situations, the solution has commonly been to provide people with machine-readable identification cards that are easy to hide and in some cases difficult to modify.

Since the 1970s, magnetic-stripe credit cards have been a standard method of automated identification. Magnetic stripes are technologically similar to audiotape in the sense that data is recorded on a special surface by applying a magnetic field to it and later played back by passing it over a magnetic sensor. At the time of the introduction of magnetic stripes on credit cards, scanners to read them were sufficiently rare and expensive that it would be challenging to read cards in an unauthorized manner or tamper with the magnetic media. Now, however, magnetic stripes are used in many new settings, such as on driver's licenses, student IDs, conference passes, store loyalty cards, and room keys, resulting in a large market for reading and writing hardware. Magnetic stripe readers and writers are relatively inexpensive (about $500) and do not require expert knowledge in order to use them. This creates a situation in which the magnetic stripe is now easier to modify than the printed information on a card.

Both bar codes and magnetic stripes are limited by the fact that they store only a small amount of information. As a result, bar codes and magnetic stripes usually store little more than an ID number that links to a full data record elsewhere in a database. As a result, smart-card AIDC systems have been developed to allow for large quantities of information to be stored on the card itself. Smart cards are in fact small computers and do not need to point to an entry in a remote database in order to reveal meaningful information. The risk of tampering still exists, but encryption techniques make this task very difficult, if not impossible. Smart cards are similar in appearance to a magnetic stripe card, but they are distinguished by a small square containing gold electrical contacts that connect to a computer inside the card.

When inserted into a scanning machine, the card's internal memory can be read and modified. The bidirectional communication between the computer inside the card and the reader allows for sophisticated interaction, which enables each to

verify that the other is a valid device authorized to perform its task. As a result, a smart card can provide reasonably secure storage of electronic cash, medical data, or other information that the designer wishes to control.

Because the magnetic stripe or smart card is not permanently affixed to the person being identified, cards may be exchanged or stolen, leading to misidentification. To ensure that the cardholder is the intended user, various techniques have been used to match the owner with the card. Two approaches are to require a signature when the card is used (which must match a signature on the card) and to put a picture of the person on the card (which must match the person using the card). Neither method provides very strong security, and the matching procedure in both cases must be performed by a person. To address this problem, biometric information has been included in the electronic data of the card. In the context of security and AIDC, biometry focuses on the computational analysis of features that identify individuals. To match ID cards to their owners securely and automatically, the favored metrics are the nearly unique patterns found in fingerprints and iris blood vessels. Other less common techniques are voice analysis and face recognition. Whichever metric is used, a few features nearly unique to the cardholder are stored in the card's memory. A person attempting to use the card later is subjected to analysis to determine if his or her features match those stored on the card.

AIDC is concerned with reducing the human effort involved in identifying objects and people, but all of the technologies described so far require an explicit scanning act that is labor intensive. Radio frequency identification (RFID) is an extension of the smart card concept in that it consists of devices that can securely read and write to special electronic tags. The main innovation of RFID is that it employs wireless communications to eliminate the need for the card reader to physically touch the card. In fact, scanning can occur without any human operator at all, since the tag simply needs to pass within the vicinity of the reader. The RFID tags or transponders can be physically smaller and less expensive to produce than an ID card, making them suitable in many applications in which bar codes have previously been employed. The reading distance for RFID tags depends on the application and underlying technology, but it ranges from several centimeters to several meters. Current uses include automated payment for public transport, road tolls, gasoline, and fast food; tracking of parts in factories and warehouses; livestock and pet identification; building access cards; and medical patient IDs. The retail chain Wal-Mart and the U.S. military are pushing their main suppliers to put RFID tags on products. As they become commonplace, RFID systems will uniquely identify the items that they are attached to and, by extension, may identify the person holding or wearing them. The push for faster, less labor-intensive, and more convenient retail checkout and inventory control has created the potential for new, hidden forms of surveillance of individual people.

AIDC and the U.S. Driver's License

A driver's license is currently the most requested form of identification in the United States, making it a prime target for integration with AIDC technology. This card, issued by state Departments of Motor Vehicles (DMVs) to certify a person's right to drive a car, has become the means by which individuals are granted access to a wide range of unrelated activities such as writing a check, buying a drink, or boarding a plane. Retailers, government agencies, commercial airline companies, and others who depend on the driver's license for personal identification look to AIDC technologies—like the magnetic stripe, bar code, or smart card—to automate and secure this process. With the addition of AIDC technology, the driver's license does not simply enable quick and trustworthy identification; it also enables retailers, agencies, and commercial businesses to collect massive amounts of data about a person, information that accumulates each time the card is provided.

Companies and government agencies that want to collect data from driver's licenses run into difficulties, however, because no uniform industry standards currently exist. Since licenses are not federally regulated, each state determines how it issues and monitors the licenses it produces. Therefore, a driver's license in Maine does not look like a driver's license in Utah, and frequently driver's licenses within a state vary greatly because states have changed standards over the years. Currently forty-six states are using some type of magnetic-stripe or bar-code technology (or a combination of both), with the remaining four states actively considering or making plans for implementation.[3] Not only do the basic card technologies vary from state to state, but also the methods for encoding the information differs, making universal reading impossible. To make matters more confusing, the amount and type of information encoded are irregular as well: in some states, the electronic information on the magnetic stripe or bar code just mirrors the printed information on the front side of the card, while in other cases additional information such as Social Security numbers, digital fingerprints, and face recognition templates augment the standard information.

The American Association of Motor Vehicle Administrators (AAMVA), a lobbying organization for the state motor vehicle administrations, has been pushing to change this situation, citing it as a threat to national security and an inconvenience to corporate America.[4] In the post-9/11 climate, the AAMVA's call for a universal standard is finally making material progress and gaining vocal support from industry leaders such as Larry Ellison of Oracle and important government officials such as Tom Ridge, the former director of the Department of Homeland Security. Any proposal that remotely resembles a national ID plan has been routinely shot down in the United States, initiating intense criticism from both political parties. In the current crisis of "permanent war," however, traditionally unpopular policies are able to gain peer support by promising a new sense of security. Another example of politi-

cal policy remaking that gained momentum through 9/11 security rhetoric is the recent Intelligence Reform Bill. This allows for data sharing and increased contact between intelligence and law enforcement agencies, something strictly prohibited since the 1970s when the FBI's counterintelligence programs and overreaching surveillance techniques became public.

In May 2002, the AAMVA plan got its biggest boost: Representatives James Moran (D-Virginia) and Tom Davis (R-Virginia) introduced HR 4633, or the Driver's License Modernization Act of 2002, which reflects AAMVA's recommendations and establishes national standards for state issuance of driver's licenses.[5] These standards include the implementation of smart-card technology to store personal information, including biometric data, and a centralized database of U.S. driver's license information. Supporters of this legislation consistently state the primary goal to be, of course, secure identification, but already secondary functions are being proposed, such as using the smart card on the driver's license to administer food stamps and voter registration.[6] This legislation would establish the driver's license as an apparatus for total and automatic authentication, analysis, and control. If HR 4633 becomes law, driver's license swiping will no longer be an infrequent occurrence but an expected consequence of participation in American society.

Who Is Swiping Driver's Licenses Today?

Government officials as well as private businesses are already using computer hardware to read the information from a driver's license magnetic stripe or bar code, the police being among the first to do so. When stopped for speeding, for instance, a driver must show his or her driver's license. Previously, a police officer would call information into headquarters. Today, it is more likely that he or she will take the card back to his or her vehicle, swipe it through a dashboard-mounted scanner, and cross-reference the information using several databases such as the National Crime Information Center (NCIC) or the National Law Enforcement Telecommunication System (NLETS). Instantly the officer will find out, for example, if the driver has a past record of driving offenses or a criminal record. Coplink, a database system allowing American police officers to instantly access and exchange information, has been specifically designed to facilitate this procedure.

Liquor and tobacco stores, as well as nightclubs and bars, were the first commercial businesses to realize the benefits of such systems. These businesses, required by law to verify age, turned to license-scanning hardware to automate a necessary function. As we have seen, however, the real motivation for purchasing and maintaining such a system may not be for the purposes of efficiency or to uphold the law more effectively but, instead, to build a detailed and valuable customer database virtually free of charge. In all but two states (New Hampshire and Texas), there are no restrictions against storing the data once it has been read from a license. Companies

selling the hardware make data collection as easy as possible for their customers by bundling customer database software with their products.

The software that comes with the license scanners makes explicit what businesses might do with the data once it is collected. Typically this software allows businesses to accomplish many different goals: it can archive customer information and transaction history in a database; parse data based on keywords; analyze customer transactions based on demographics or customer statistics; export data to use in other applications; print letters, labels, and reports; and set alerts for specific individuals, so that when their IDs are scanned, a message is displayed in real time.[7] Any business would find value in such software, while the most obvious benefit is for fulfilling marketing purposes. A database is valuable for other reasons as well, such as analyzing a customer base for strategic planning or providing data to investors in order to justify future projects.

There have been only a few instances in which states have stopped the practice of driver's license swiping with legislation, and this was usually in response to a citizen protest that the practice violated the Driver's Privacy Protection Act.[8] There are, however, persuasive reasons why government would allow the practice to continue and turn a blind eye. Law enforcement, for instance, from the local to the federal level, reaps huge benefits from commercial businesses that collect transaction data because it can be used for investigations and subpoenaed at a later date. Most recently, in the so-called war on terror, federal agents have requested transaction histories from businesses such as bookstores and shops that sell scuba gear. The more the information is detailed, organized, and electronic, the easier it is for the agents to request, receive, and utilize the data. Weeks after 9/11, a supermarket voluntarily handed over its customer database complete with purchase histories to federal investigators. This was not in response to a request, a spokesperson for the store contended, but rather appears to have been some kind of patriotic gesture.[9]

Furthermore, the use of AIDC technology has become so widespread that government officials are not only using it to request data in pursuit of committed crimes but are also employing it to establish databases from commercial transactions in case of *future* criminal behavior. One such example is occurring in the state of Pennsylvania. When an ID is scanned at a Pennsylvania state-run liquor store, the purchase and identification information is added to the Pennsylvania Liquor Control Board's (PLCB) electronic database in Harrisburg.[10] The PLCB database is preemptive: it was established to assist police with criminal cases that have yet to be committed. In order to grant the police this comfort, however, every Pennsylvania resident's alcohol purchase history is monitored and recorded. Because it is not possible to buy bottled wine or spirits in Pennsylvania at any place other than a state-controlled liquor store, there are no options for circumventing this surveillance unless a person buys liquor out of state. License scanners have been used in

Pennsylvania liquor stores since 1997 and are currently installed in all 638 state-run liquor stores.

Airports, hospitals, and government buildings are the latest places that use driver's license scanners, as the *New York Times* reported in 2002. "Logan Airport in Boston is using [driver's license scanning] machines to check the identity of passengers. New York University Hospital scans and stores visitors' driver's license information. Delaware has installed the machines to screen visitors at the state legislature and its largest state office building."[11] With most DMVs issuing data-encoded driver's licenses and with the cost of driver's license scanning equipment so low that even novice computer users can manage them, many businesses and government agencies are adopting or considering carding and collecting personal information.

Driver's License Swiping and Digital Data: Hidden Information and Database Mistakes

License scanning usually occurs outside the cardholder's field of vision. Police officers are taking the driver's license with them to run a quick check inside their car. Card scanners at convenience and liquor stores are often placed underneath the counter and are invisible to the customer. Even if a customer sees the driver's license scanner in use, it does not necessarily make the process transparent: not only might the customer not realize what is happening but he or she generally does not know what information is stored on the card, nor does he or she know what will be done with the information after it is collected. If a customer does ask what the store is going to do with this information, often attending clerks will simply shrug their shoulders. Employees are not usually trained to understand the ways in which their store database operates. Customers are thereby left powerless vis-à-vis their personal information, now entered into a computer system whose purpose and functions remain opaque to them. The situation does not allow for a helpful exchange of information. There is no chance to opt out or even verify that the information is correct.

Human errors resulting in false entries are not uncommon. In the case of a driver's license record, a person's file begins after an employee at the DMV enters information by hand into a database from a form, which ultimately ends up encoded on the driver's license. Mistakes, of course, happen; it is only human. In our experience scanning people's driver's licenses, we have seen cards in which the information on the front is correct, while the digitally encoded data on the back is different and false. Yet once the entry is made and travels to other databases, the false data acquires legitimacy by mere fact of replication. Sometimes database mistakes do not result from mistyping but, rather, from identity confusion. If two people's names are similar or they have nearly identical Social Security numbers, their information can easily be scrambled. The U.S. Public Interest Research Group's (PIRG) study on credit reports, for instance, found that 70 percent contained errors and 29 percent

were the result of reporting credit accounts that belonged to another consumer.[12] When mistakes are found, individuals are faced with the nearly impossible task of tracing the source of the error and rectifying the mistake across numerous databases. Substantial amounts of time, money, and knowledge are needed to complete this tedious task.

Data warehouses, that is, businesses that consolidate data from various sources and resell it to third parties—are at risk for perpetuating false information. These companies should, one would imagine, pay considerable attention to verifying all data they redistribute, but unfortunately this is not often the case. ChoicePoint, a well-known data warehouse based in the United States, is aware of its own data flaws and therefore does not assume liability for the accuracy of its information.[13] This seems particularly disturbing since ChoicePoint is the leading commercial supplier of information to the U.S. federal government. It has multimillion-dollar accounts with thirty-five different federal agencies, including the FBI, the IRS, and the Department of Justice. In 2002, ChoicePoint was ultimately held accountable for its poor verification practices by a New York court and ordered to pay $450,000 to the plaintiff.

ChoicePoint does offer individuals the chance to review what information is maintained about them in its database for a fee of twenty dollars. The privacy expert David Smith did just that and found that it contained more inaccurate than accurate information and learned later that he could not opt out from the ChoicePoint's collection of personal data.[14] ChoicePoint suggests that if a person finds inaccurate information in his or her files, he or she should contact the originator of the data to correct the problem, pointing a person toward the labyrinth of public offices, commercial businesses, and credit agencies from which the data originates.

The Rhetoric of Convenience versus Privacy

More than fifty years after George Orwell's *Nineteen Eighty-Four* was published, *Big Brother* is still the most dominant metaphor used in popular culture to describe surveillance societies. Today, at least in the case of the United States, this metaphor is less useful and even misleading in the description of contemporary surveillance societies. As David Lyon puts it, "Orwell's dystopic vision was dominated by the central state. He never guessed just how significant a decentralized consumerism might become for social control."[15]

The examples we have outlined so far—as with most AIDC technologies—are not matters of state coercion but rather consensual situations in which an individual willingly participates (most often through consumption) and as a result submits to some sort of commercially controlled surveillance system. This condition is often referred to as convenience versus privacy. People are led to believe that when they use the latest technological innovations (cell phones, E-ZPass tags, supermarket loyalty cards), the benefits inherently come with unpleasant surveillance possi-

bilities and that modern luxuries have strings attached. Modern luxuries, of course, quickly transition into necessities, and with the proliferation of AIDC technologies even basic pleasures—like buying a bottle of wine—present a person with the dilemma of convenience *or* privacy.

The E-ZPass is one such modern luxury that raises the convenience-versus-privacy issue for many people living in the Northeast region of the United States. The E-ZPass is an optional device that a person affixes to his or her car windshield that triggers automatic debit from an electronic account when driving through a highway tollbooth. The convenience is that one has much less of a wait at a given tollbooth. This particular electronic toll-collection system (which is not unique to the United States) consists of a RFID tag that transmits a unique ID from the car to the RFID receiver in the toll lane. This information is transferred to a customer database to debit the cost of the toll from the customer's account. Along with account balance information, the database also records location, time, and toll lane. Other factors like average speed can be interpolated using two points of entry in the database. This rich information has not only been used for debiting accounts but also for policing purposes such as issuing speeding violations and increasing car insurance fees.[16]

There is, of course, no reason that E-ZPass tags *have* to be unique to drivers. They could function instead, for instance, more like disposable phone cards that are available at most convenience stores. This card would be bought with a set amount of dollars, decreasing with each use and ultimately becoming invalid when it reaches zero. State transportation departments would still benefit from this automatic debit system (as they do now with E-ZPass information), using anonymous data to conduct surveys of traffic patterns for future highway improvements. However, this disposable E-ZPass system would not grant policing and control powers through unique RFID tags to the company that owns the E-ZPass. The disposable system would therefore eliminate the convenience versus privacy dilemma by granting convenience without increasing corporate control.

Government and Corporate Codependence

This E-ZPass scenario not only illustrates how corporations are increasingly becoming policing forces through the use of new technologies but also demonstrates the ways in which a private business (E-ZPass) shares data with a government body (state transportation departments) for a common cause (to improve congestion problems through E-ZPass integration into the highway system). This type of data sharing between the private and public sectors for the benefit of both parties is not uncommon or limited to AIDC technologies. Another recent example involved the turnover of Jet Blue Airlines' customer records to the Transportation Security Administration (TSA). Jet Blue released its customer data on request and without notifying

or receiving consent from the subjects involved, something in clear violation of its own privacy policy. The TSA wanted the information for a data mining experiment whose purpose was to assess the terrorist risk of each passenger record.[17] Such tactics leave customers with the uneasy feeling that data originally collected for one reason can easily be used for others without their knowledge.

There are other instances, as we have seen with ChoicePoint, in which the *entire purpose* of a business is to provide the government with information. Here, the motivating factor is not a common public-private collaboration, but revolves almost exclusively around profit. The government, for example, does not typically seek out commercial warehouses because they have access to special information; ChoicePoint's data is drawn from public records combined with information provided by the media, credit-reporting firms, and, in some cases, private detectives. Often government agencies turn to private companies and outsource data-collecting jobs to circumvent the Privacy Act of 1974. This law places restrictions on the collection, use, and dissemination of personal information by and between government agencies, but it never set limits on the private sector. Even after the passage of the USA PATRIOT Act in 2001, which legalized enhanced government data collection and analysis with reduced checks and balances, the government still relies on the private sector to perform "watching" activities at full speed.[18]

Perhaps the most questionable use of commercially maintained data by the government sector in recent years occurred in 1998 when the Florida state legislature made an unprecedented decision to scrub ineligible voters—mostly ex-felons—from the state's voter registration list based on information bought from a commercial firm. The state legislature claimed this as the necessary response to a botched Miami mayoral race in which numerous illegal votes were cast. But the 4 million–dollar contract went to ChoicePoint, and it is estimated that thousands of voters—disproportionately black—were unduly disenfranchised in the 2000 presidential election as a result of faulty, unverified data.[19]

Data flows, of course, in the other direction too: from government body to corporate database. Private businesses for a long time now have used census data and other public records that are made free and available by the U.S. government to make decisions about future store locations or product pricing. This practice of using characteristics like age, gender, or income for market research is called demographics. With the increase in data storage capacities and the ease of accessing public information through the Internet, demographic analysis has become massively accelerated. This type of commercial use of public information dramatically undermines its original purpose. Data made available to make government bureaucracies more visible, and thus accountable, to its citizens is instead being used by businesses to study its consumers in search of increased corporate profits.

Consequences of AIDC

In light of new technologies, including AIDC, there is an urgent need for broader reconsideration of data collection and usage practices in the United States. The data situation is already dire (as our examples suggest) and in danger of getting exponentially worse. AIDC does not create a bad situation, but it aggravates one that remains without sufficient controls (technological or governmental) and without satisfactory public understanding to allow for a just implementation. An in-depth discussion of AIDC's social implications lies beyond the scope of this essay, but we would like to underscore a few examples, specifically considering AIDC's role in intensifying consumer profiling and creating fear or a sense of permanent guilt.

Consumer profiling is the recording and classification of behavior through aggregating data. Consumer profiling is related to demographics, but it targets an individual based on specific, nonanonymous data that is sometimes bundled with more general information like census data. Loyalty cards used in grocery stores, for instance, allow for the collection of individual purchase information that is analyzed and ultimately used for direct marketing. Consumer profiling refines a store's marketing strategies and profits; the consequences are typically junk mail or individualized coupon discounts during checkout at a grocery store. While this type of mail or coupon may be desired in some instances and annoying in others, the important aspect is not the extra offers made to a specific group of people, but rather the limited choices for people outside the target group. Boundaries between income groups and other store-determined clusters are created and reinforced, and they become pronounced over time. Whereas this phenomenon is not new and occurs with or without the existence of AIDC, loyalty-card data certainly accelerates and individualizes this process.

Many people think these store loyalty cards produce great savings, and opposition to enrolling is met with, "Why, do you have something to hide?"[20] Most of us do not think we have anything to hide, but you never know anymore, as was the case of a man who, while shopping at Vons grocery store, slipped and fell on some spilled yogurt.[21] When he tried to sue the store to recover for lost wages, pain, and suffering, Vons threatened to use information from his loyalty card records against him in court. The store claimed that the customer bought an inordinate amount of alcohol. It was later determined that alcohol was not a factor in the incident, and the threat by Vons was ultimately dropped. The underlying message, however, is clear: your data bits can be selectively used to paint a certain data biography (or support a particular point of view), and the potential for a person's past data to be used to intimidate him or her—even when the data is fairly innocuous—always remains a distinct possibility.

There are many times, of course, when the data is not innocuous, but actually very sensitive. This was the case in *Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA)*, in which a doctor guaranteed a patient (Doe) that

his health insurance company (SEPTA) would not inquire about the prescription drugs he was using to treat his HIV. Although SEPTA did not ask, Rite-Aid pharmacy supplied it with a list of his drugs anyway. Doe's doctor informed him of this mistake, and Doe feared his employer (who paid for the insurance) was ultimately in the know too. Doe filed a lawsuit, but the court decided that his privacy invasion was minimal. As Daniel Solove comments, "[The court] missed the nature of Doe's complaint. Regardless of whether he was imagining how his co-workers were treating him, he was indeed suffering a real palpable fear. His real injury was the powerlessness of having no idea who else knew he had HIV, what his employer thought of him, or how the information could be used against him. This feeling of unease changed the way he perceived everything at his place of employment."[22]

This situation underscores the way people relate to their own data: removed, unsure, and powerless. Those who work inside the bureaucracy are often unsure, too, which leads to harmful mistakes and the likelihood that information can end up in the wrong hands. If AIDC technologies are utilized to administer health benefits (as is the case in Canada and as has been proposed in the United States), no trustworthy systems are in place to handle the flow of sensitive information. In the United States, personal medical information is, in fact, so unprotected that businesses such as the Medical Marketing Service exist for the sole purpose of selling lists of persons suffering from various ailments. To employ any technology that would further ease the distribution of sensitive medical information in the United States would be unwise until more safeguards are built into the health and judicial systems.[23]

AIDC technologies facilitate not only the collection of personal information for immediate analysis and use but also the archiving of information as a way to monitor the subject in case of future wrongdoings. This aspect of AIDC technologies can be called "guilty until proven innocent." This is certainly true in the case of the Pennsylvania Liquor Control Board, which records every individual sale of liquor and wine in Pennsylvania in a separate database in anticipation of future crimes associated with drinking. One of the authors of this paper was encouraged to participate in a similar guilty-until-proven-innocent program while an employee at a museum. In the aftermath of several thefts, the museum proposed fingerprinting each staff member, telling employees that this would automatically rid them of implications in future problems. In essence, the museum was telling its staff that it trusted none of them and that only fingerprint data would totally clear their names of future crimes. AIDC technologies were not implemented at the museum, but the administration's attitude is a common reason companies turn to and employ AIDC technologies in the first place. This is a new condition in American life: people are held in suspicion until they can offer data to prove their innocence.

One place Americans are now used to being treated with suspicion until they provide an ID, answer some questions, and get frisked is the airport. After 9/11,

airport security in the United States has been reviewed and tightened. Some of these changes make sense. The prohibition against a person boarding a flight with a small knife or box cutters could indeed further flight security without impacting a passenger's freedom of movement. But passenger profiling, and, more specifically, the second generation of the Computer Assisted Passenger Pre-screening System (CAPPS II), requires closer review and is riddled with problems similar to those we have raised concerning AIDC technologies. CAPPS II is a data-driven system that electronically absorbs every passenger reservation, authenticates the identity of each traveler, and, finally, creates a passenger assessment. The project, overseen by the TSA, is a data-matching project (rather than a data-mining project), which means that passenger information is verified against external databases to determine that people are who they say they are (identity verification) and to assign them a terrorist risk level (assessment). In this system, passengers are required to provide identifying information when making a flight reservation such as name and address, a passport, and their Social Security and frequent flyer numbers. These details are then cross-referenced with information provided by private data firms. The end result: each traveler receives a threat assessment color. In this system, green means "fly freely," yellow means "extra security checks," and red means "not allowed on board." The Department of Homeland Security urged the use of this program on all commercial flights originating in the United States by the summer of 2004 and has supposedly been testing the program on select Delta Airlines flights since spring 2003.

CAPPS II, as far as we can tell based on the little information released to date, would provide the government with a central control mechanism capable of restricting a person's movement within the United States. A tool of this magnitude represents a major threat to civil liberties. The government can at any time change the system's parameters (who is targeted and when), immediately influencing the lives of millions of citizens. A person in the unfortunate position of being included in a target group could experience serious impacts with no justification. For example, a woman who relies on air travel for a living could lose out professionally if she is detained often and misses meetings. Faced with such a problem, the businesswoman could not inquire why she was being targeted and how she might clear her name since, as of now, the U.S. government has no system in place for a person to contest an evaluation he or she perceives to be in error. Furthermore, the methods used for verifying data and for what rules determine the final threat assessment are not disclosed. Of course, officials claim that for security reasons the process must remain top secret. However, if the government is controlling who can move freely in the country based on an automated system with unverified data, this will not offer any real security. It can only lead to disaster and misuse.

Awareness Raising, Approaching Solutions

So far, we have attempted in this essay to give an overview of AIDC technologies and draw attention to some of the related social implications. However, as tactical media practitioners and interdisciplinary artists, we are interested in developing projects that use communicative means other than the written word to address our concerns. Swipe—a three-part project consisting of a performance, a workshop, and a Web site—has been our participatory response to the various controversies affiliated with driver's license swiping and data collection.

The Swipe project is primarily educational in that it informs citizens of a particular practice and offers an opportunity for public discussion. The performance centers on an alcohol-serving bar from which a person gets a drink and an unusual printed receipt. The receipt contains all the information we swiped from his or her driver's license at the point of sale, plus any additional personal information we could glean off the Internet and archived databases while the customer's drink was being prepared. The workshop offers a demonstration that demystifies the data collection and data warehouse businesses, offering a behind-the-scenes look at the Swipe bar. The Web site, launched in February 2004, offers a set of hands-on tools for the motivated cultural activist. On the Web site, users can decipher the two-dimensional barcode on a driver's license through a downloadable program, determine the value of personal information on the open market using a data calculator, and request a data file from big data warehouses such as ChoicePoint. Using a bulletin board system, users can post how many errors appear in their requested files and keep track of the response time of the data warehouses to correction requests.[24]

Education and raising awareness are, of course, very important. Only with understanding can there be public reaction, and only due to persistent public outrage will there be a reason for government and industry to change practices. Resistance on the individual level is also helpful. Some common strategies are paying with cash instead of using the E-ZPass or using another customer's loyalty card to add noise to the store database. As part of Swipe, we distribute stickers for people to place over their magnetic stripe or bar code on drivers' licenses that have slogans such as "Keep your paws off my databody" or "I stop shopping when you start swiping." These stickers temporarily disable the AIDC technology and will ensure that a person's information is not swiped without notification or consent. These stickers have the potential to create an interesting situation when a shopkeeper, police officer, or bouncer notices the sticker and has a moment of recognition (verbal or nonverbal) with the cardholder.

In terms of long-term solutions, we feel the answers must be found in both technology and policy. There are technological fixes to some of the data collection problems we have raised. For instance, Latanya Sweeney's research into computational disclosure control has produced several software programs that remove individual's names and other unique identifiers from a database without rendering all

the data useless for research purposes. There are, of course, times when identifying an individual may be necessary; Sweeney comments, "Despite the possible effectiveness of these systems and others not mentioned here, completely anonymous data may not contain sufficient details for all uses, so care must be taken when released data can identify individuals and such care must be enforced by coherent policies and procedures. The harm to individuals can be extreme and irreparable and can occur without the individual's knowledge. Remedy against abuse however, lies outside these systems and resides in contracts, operating procedures and laws."[25] The contracts, operating procedures, and laws Sweeney mentions should be considered and developed *alongside* emerging technologies. The privacy policies in the United States have been written in response to failures in the system and work as patches to immediate problems. These fixes are never complete and are often too easy to work around or ignore all together. Rights of privacy, social justice, and equality must be addressed at the start of AIDC research and development, not tacked piecemeal onto different projects only after trouble arises.

Clearly, AIDC technologies are economically attractive: they reduce labor costs and help feed information about industrial and commercial processes directly into computers that can further streamline those systems. When the target of AIDC is the consumer, massive databases are created that in turn can be used in an attempt to model human behavior to predetermined demographic cluster groups, medical conditions, and allegedly terrorist inclinations. Due to the current legal and political environment, data determinism is flourishing, and any perceived protections against this kind of activity are simply illusory. Our goal has been to describe AIDC and highlight how it encourages a broad range of data surveillance activities that have been subject to increasing criticism. We hope that this perspective can benefit participation against new forms of surveillance, in legal, political, and activist settings.

Notes

1. This assumption is wrong. See "The AIDC Industry and Technologies: A Technical Overview" in this article for more elaboration.
2. Dan Wiederer, "Answering Age-Old Questions," excerpt from tobacco retailer, June 2002, www.cougarmtn.com/news/featureArticle/tobaccoRetailer_Jun02.asp.
3. For a reference table issued by the American Association of Motor Vehicle Administrators (AAMVA), please see "Current and Planned Technologies for U.S. Jurisdictions," at the AAMVA Web site, www.aamva.org/standards/stdUSLicenseTech.asp (accessed November 30, 2003).
4. AAMVA, "AAMVA Helps Secure a Safer America," January 14, 2002, www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp (accessed November 30, 2005).
5. The bill summary and more information about the Driver's License Modernization Act can be found at thomas.loc.gov/cgi-bin/bdquery/D?d107:4633:./list/bss/d107HR.1st::/TOM:/bss/107search.html (accessed December 18, 2005).

6. William Welsh, "Driver's License Bills: Reduce Speed Ahead," *Washington Technology*, August 23, 2002, www.washingtontechnology.com/news/17_13/statelocal/18969–1.html.
7. The online manual for TriCom's "Visitor Manager Software," a product sold along with its ID-E handheld driver's license reader, describes these capabilities. TriCom Card Technologies, "Visitor Management Software Introduction," www.tricomcard.com/manuals (accessed December 19, 2005).
8. Karen Dandurant, "License Scanning, Now Illegal," *Seacoast Online*, May 3, 2002, www.seacoastonline.com/2002news/exeter/05032002/news/2731.htm.
9. Erik Baard, "Your Grocery List Could Spark a Terror Probe, Buying Trouble," *Village Voice*, July 24, 2002, www.villagevoice.com/news/0230,baard,36760,1.html.
10. William Berry, "Cops Use ID Info in Criminal Cases," *Digital Collegian*, April 9, 2003, www.collegian.psu.edu/archive/2003/04/04–09–03tdc/04–09–03dnews-08.asp.
11. Jennifer Lee, "Welcome to the Database Lounge," *New York Times*, March 21, 2002.
12. Jon Golinger with Edmund Mierzwinski, "Mistakes Do Happen: Credit Report Errors Mean Consumers Lose," March 1998, uspirg.org/uspirg.asp?id2=5970&id3=USPIRG (accessed December 19, 2005).
13. ChoicePoint Privacy FAQs can be found at www.autotrackxp.com/privacy_faqs.htm#correct (accessed November 30, 2003).
14. Electronic Privacy Information Center (EPIC), "Epic Digest at Privacy.org," May 8–15, 2001, www.privacy.org/digest/epic-digest05.15.01.html. Privacy.org is a joint project of EPIC and Privacy International.
15. David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994), 78.
16. The friend of one of the authors moved from upstate New York to New York City and did not immediately notify his car insurance company of his move. He subsequently bought an E-ZPass for his work commute—a drive he began to make on a daily basis. Within weeks of his move, his car insurance company sent him a notice informing him that his insurance rate was more than doubling based on his new residency. When he called the car insurance to discuss the fare hike, he asked how they knew of his move. The operator told him that it was based on E-ZPass data the company routinely acquired. For E-ZPass FAQs, see www.ezpass.com/static/faq/speed.shtml (accessed November 30, 2003).
17. "Betraying One's Passengers," *New York Times*, September 23, 2003.
18. Electronic Frontier Foundation, "The EFF Analysis of the Provisions of the USA Patriot Act That Relate to Online Activities," October 27, 2003, www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.
19. Gregory Palast is a journalist who extensively investigated this incident. See his "Florida's Flawed 'Voter-Cleansing' Program," *Salon*, December 4, 2002, archive.salon.com/politics/feature/2000/12/04/voter_file/print.html.
20. The fact that these cards save money was proven untrue. See Katy McLaughlin, "The Discount Grocery Cards That Don't Save You Money," *Wall Street Journal*, January 21, 2003.
21. Jennifer Vogel, "Getting to Know All about You," *Salon*, October 14, 1998, archive.salon.com/21st/feature/1998/10/14featureb.html.
22. Daniel Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stanford Law Review* 53 (2001): 1438.
23. To read more about medical data and privacy issues in the United States, see Latanya Sweeney's research at privacy.cs.cmu.edu.

24. Please see the authors' Web site, www.we-swipe.us, for a full project description and documentation.
25. Latanya Sweeney, "Privacy and Confidentiality, in Particular, Computational Disclosure Control," Carnegie Mellon University Data Privacy Lab, privacy.cs.cmu.edu/people/sweeney/confidentiality.html (accessed November 30, 2003).