

Introducing AIDC as a Tool for Data Surveillance

BEATRIZ DA COSTA+JAMIESON SCHULTE+BROOKE SINGER

Introduction

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 licence — the usual procedure in the United States for any person who looks under 30. The woman hands over her licence 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 licence 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 licence, but for the first time she notices a magnetic stripe on its backside very similar to her credit card.

A number of thoughts run through her mind. Why didn't he just look at the face of the licence 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 inspired us to take a closer look at driver's licence card technologies and the industry family to which they belong — Automatic Identification and Data Capture technologies (AIDC). The purpose for using magnetic stripe technology, and for AIDC technologies in general, is to identify people or objects through machine automated processes. But why is AIDC technology even necessary for such a simple task as verifying a person's age in a liquor store? Why are technological solutions cropping up in the most routine tasks of our everyday lives?

The liquor store would 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 tallies up the customer's age; a machine quickly does it for him. The store would also claim that a magnetic stripe is much harder to tamper with than the face of the driver's licence, making fraudulent IDs easier to detect.¹



Both efficiency and fraud prevention ultimately save the business money. Every store wants to serve customers as quickly as possible and a liquor store especially 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. ID verification 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 "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 which is nearly free of charge and exactly describes a business customer base, is arguably the most important benefit a card-verification system brings to a business — and in some cases the U.S. government as well.

This paper explores current and proposed uses for AIDC technologies, focusing primarily on the already widespread practice of driver's licence swiping in the United States. Driver's licence swiping is an ideal case in point and it 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 'surveillance creep' into every facet of contemporary life.

We begin with a technological discussion. It is our belief that critical assessment of, and informed reaction to, AIDC must be founded on solid technical knowledge. Our aim is not to denounce all AIDC uses, but to bring about a better understanding of this vast and rapidly developing field, which is often in conflict with our ideas of social justice. More public consideration of these technologies will help shape a better future with AIDC technologies that, in our opinion, must incorporate safeguards built into the technology itself, coupled with better governmental policy controls.

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 now include retail check-out, warehouse inventory, livestock management, vehicle drivers' licences, 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 labour 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. This information represents a high value for a number of businesses and has opened new markets, such as data collection and data selling.

AIDC addresses an old technological problem: how can a computer identify an object in the real world? As of 2003, computer vision research has not yet come close to producing systems that can visually recognize a wide range of objects in a natural environment without significant error. Even if vision worked well, a computer would be unable to differentiate between different objects that have the same appearance. To reduce this problem, AIDC focuses on techniques that involve 'tagging' objects with a 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 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 labour.

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 since most products are already marked with a UPC symbol, but they require careful scanning by a human operator.³ More advanced encoding schemes, often called 2-dimensional bar codes, consist of a square region filled with small black and white pixels and can represent a greater quantity of information. 2D bar codes are used on some ID cards, by the U.S. military, and have been adopted as the national standard for bar coding by China.

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 students⁴ 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 audio-tape, 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 their introduction on credit cards, magnetic stripe scanners 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 drivers' licences, 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 can be purchased on a personal budget (about \$500) and don't require expert knowledge to be used. This creates a situation in which the magnetic stripe is now easier to modify than the printed information on a card.

In addition to security concerns, 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 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 bi-directional communication between the computers inside the card and the reader allows for sophisticated interaction, which enables each to verify that the other is a valid device that is 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 (1) to require a signature when the card is used (which must match a signature on the card), and (2) 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 favoured 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 that are 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



labour-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 where bar codes have previously been employed. The reading distance for RFID tags depends on the application and underlying technology, but ranges from several centimetres to several metres. 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 by 2005. 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 labour-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 Licence

A driver's licence is currently the most requested form of identification in the U.S., making it a prime target for integration with AIDC technology. This card, issued by state Department 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 (writing a check, buying a drink, or boarding a plane, for example). Retailers, government agencies, commercial airline companies, and others who depend on the driver's licence 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 licence does not simply afford quick and trustworthy identification, but enables retailers, agencies, and commercial businesses to collect massive amounts of data about a person that accumulates each time a card is provided.

Companies and government agencies that want to collect data from drivers' licences run into difficulties, however, because no standards exist. Licences are not federally regulated, leaving each state to determine how to issue its own. Therefore, a driver's licence in Maine does not look like a driver's licence in Utah and many times drivers' licences within a state vary greatly because states change standards.

Currently forty-six states are using some type of magnetic stripe or barcode technology (or a combination of both) with the remaining four states actively considering or making plans for implementation.⁵ Not only do the basic card technologies vary from state to state, but also the methods for encoding the information differ, making universal reading impossible. To make matters more confusing, the amount and type of information encoded is irregular: in some states the electronic information on the magnetic stripe or barcode is just a mirror of 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.⁶ 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 politicians (such as Tom Ridge, Director of Homeland Security). Industry and government officials may have desired standardization earlier, but were hesitant to voice their opinion. Any proposal that remotely resembles a national ID plan has been routinely shot down in the U.S., 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.

In May 2002, the AAMVA plan got its biggest boost: Reps. James Moran (Democrat) and Tom Davis (Republican) introduced H.R. 4633 or the Driver's Licence Modernization Act of 2002,⁷ which reflects AAMVA's recommendations and establishes national standards for state issuance of drivers' licences. 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 licence information. Supporters of this legislation consistently state the primary goal to be, of course, secure identification, but already secondary functions are being proposed, like using the smartcard on the driver's licence to administer food stamps and for voter registration.⁸ This legislation would establish an apparatus for total and automatic authentication, analysis, and control. If H.R. 4633b becomes law, driver's licence swiping will no longer be an unusual occurrence, but a precondition for participation in American society.

Who is Swiping Drivers' Licences Today?

Government officials as well as private businesses are already using computer hardware to read the information from a driver's licence 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 driver's licence. Previously, a police officer would call the information into headquarters. Today, it's more likely he will take the card back to his vehicle, swipe it through a dashboard-mounted scanner and cross-reference the data with 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 offences 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 licence-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 efficiency or to more effectively uphold the law, but 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 licence. 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 licence scanners makes explicit what businesses might do with the data once it is collected. Typically this software allows businesses to 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, or set alerts for specific individuals so when their IDs are scanned a message is displayed in real time.⁹ Any business would find value in such software and the most obvious benefit is probably for marketing purposes. A database is valuable for other reasons like analyzing a customer base for strategic planning or providing data to investors in order to justify future projects.

There are only a few instances in which states have stopped the practice of drivers' licence swiping with legislation, and this is usually in response to citizen protest that the practice violates the Driver's Privacy Protection Act.¹⁰ There are, however, good 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 'War on Terror', federal agents have requested transaction histories from businesses like bookstores and scuba dive shops. If the information is detailed, organized and electronic, the easier it is for the agents to request, receive and utilize the data. There was one reported incident in which a supermarket voluntarily handed over its customer database complete with purchase histories to federal investigators. This was not in response to a request but rather a patriotic gesture.¹¹

Government officials are not only requesting data in pursuit of committed crimes, but are also establishing databases from commercial transactions in case of future criminal behaviour. 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.¹² The PLCB database is pre-emptive: it is 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 goes to the extreme of buying out-of-state. Licence 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 drivers' licence scanners are being used. *The New York Times* reports that, "Logan Airport in Boston is using [driver's licence scanning] machines to check the identity of passengers. New York University Hospital scans and stores visitors' driver's licence information. Delaware has installed the machines to screen visitors at the state legislature and its largest state office building".¹³ With most DMVs issuing data-encoded drivers' licences and with the low cost of

drivers' licence scanning equipment that even novice computer users can manage, many businesses and government agencies are adopting or considering carding and collecting personal information.

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

Licence scanning usually occurs outside the cardholder's field of vision. Police officers are taking the driver's licence 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 licence scanner in use, that does not necessarily make the process transparent: the customer may not realize what is happening, she does not know what information is stored on the card, and she does not know what will be done with her information after it is collected.

If a customer asks what the store is going to do with her information, often the clerk will simply shrug his shoulders. Employees are not usually trained to understand the ways in which their store database operates. Customers are thereby left powerless with their personal information, having been entered into a computer system whose purpose and functions are opaque to them. The situation does not allow for a helpful exchange of information. There is no chance to 'opt out' or a chance to verify that the information is even correct.

Human errors resulting in false entries are not uncommon. In the case of a driver's licence record, a person's file begins with an employee at the DMV entering information by hand into a database from a form, which ultimately ends up encoded on the driver's licence. Mistakes, of course, happen; it's only human. In our experience scanning people's drivers' licences, we have found errors; we have seen cards in which the information on the front is correct but the digitally encoded data on the back is different and false.

Once the entry is made and follows its destiny into 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. U.S. PIRG's study on credit reports, for instance, found that seventy percent contained errors and twenty-nine percent were the result of reporting credit accounts that belonged to another consumer.¹⁴ When mistakes are found, individuals are faced with the nearly impossible task of tracing the source of the error and rectifying the error across numerous databases. Substantial amounts of time, money and knowledge are needed to complete this tedious task.

Data warehouses, businesses that consolidate data from various sources and resell it to third parties, are at risk of perpetuating false information. These companies should, therefore, pay considerable attention to verifying all data they redistribute, but unfortunately this isn't often the case. ChoicePoint, a well-known data warehouse based in the United States, is aware of its own data flaws and doesn't assume liability for the accuracy of its information.¹⁵ This is particularly disturbing since ChoicePoint is the leading commercial supplier of information to the U.S. federal government. It has multi-million dollar accounts with thirty-five different federal agencies, including the FBI, IRS and 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. The court found that ChoicePoint “intentionally maintained substandard procedures for verifying accuracy of data or should have known that its procedures were substandard under the Fair Credit Reporting Act.”

ChoicePoint does offer individuals the chance to review what information is maintained about them in its database for a fee of \$20. Privacy expert Richard 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.¹⁶ ChoicePoint suggests that, if a person finds inaccurate information in his files that he should contact the originator of the data to correct the problem and points a person towards the labyrinth of public offices, commercial businesses, and credit agencies from which the data originates.

Convenience versus Privacy Rhetoric

More than fifty years after *1984* was published, “Big Brother” is still the most dominant metaphor when describing surveillance societies. Today, at least in the case of the United States, this metaphor is less evocative and even misleading. 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.”¹⁷

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 commercial-controlled surveillance system. This condition is often referred to as ‘convenience versus privacy’. People are led to believe that by using the latest technological innovations (cell phones, EZ-Pass tags, supermarket loyalty cards) the benefits inherently come with unpleasant surveillance possibilities 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 EZ-Pass is one such modern luxury that raises the ‘convenience versus privacy’ issue for many people living in the Northeast region of the U.S. The EZ-Pass is an optional device that a person affixes to his car windshield that triggers automatic debit from an electronic account when driving through a highway tollbooth. The convenience is simply less wait at the tollbooth and more cruise time. This electronic toll collection system (that is not unique to the U.S.) 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, however, but has been used for policing purposes such as issuing speeding violations and increasing car insurance fees.¹⁸ The use possibilities for the EZ-Pass database are numerous and even unforeseeable as technologies develop and collection practices potentially change.

There is, of course, no reason that EZ-Pass tags have to be unique to drivers, but could function instead 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 invalid when it reaches zero. State transportation departments would still benefit from this automatic debit system (as they do now with EZ-Pass information), using anonymous data to conduct surveys of traffic patterns for future highway improvements. However, this disposable EZ-Pass system would not grant policing and control powers through unique RFID tags to the company that owns the EZ-Pass. This disposable system would therefore eliminate the 'convenience versus privacy' dilemma by granting convenience without increasing corporate control.

Government and Corporate Co-Dependence

This EZ-Pass scenario not only illustrates how corporations are increasingly becoming policing forces through use of new technologies, but also demonstrates the ways in which a private business (EZ-Pass) shares data with a government body (state transportation departments) for a common cause (to improve congestion problems through EZ-Pass 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 of this involved the turnover of the airline JetBlue's customer records to the Transportation Security Administration (TSA). JetBlue released its customer data to the TSA upon request and without notification or consent by the subjects involved, which was 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.¹⁹ Such tactics leave customers with the uneasy feeling that data originally collected for one reason can easily be used for other reasons without their knowledge.

There are other instances, as we have seen with ChoicePoint, in which the entire purpose of a business is to provide government with information and the motivating factor is not a common cause but rather profit. The government 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 never set limits on the private sector. Even after the passage of the USA Patriot Act in 2001, which legalizes 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.²⁰

Maybe the most questionable use of commercially maintained data by the government sector in recent years was 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 was the necessary response to a botched Miami mayoral race in which numerous illegal votes were cast. But the \$4 million 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.²¹

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 US government to make decisions such as where to put a store or how to price a product. 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 accelerated. Today businesses can utilize this information quickly, efficiently, constantly, and automatically.

Recently another commercial trend has emerged that is dramatically undermining the original purpose of public information, which was to make powerful government bureaucracies accountable to citizens. Daniel Solove, an expert in information privacy law, explains: "A growing number of large corporations are assembling dossiers on practically every individual by combining information in public records with information collected in the private sector such as one's purchases, spending habits, magazine subscriptions, web surfing activity, and credit history. Increasingly, these dossiers of fortified public record information are sold back to government agencies for use in investigating people".²² Solove suggests that regulations of public records must be rethought—including commercial access and use restrictions—in light of new technologies in the Information Age.²³

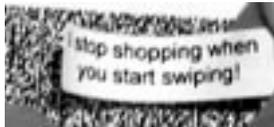
Consequences of AIDC

Similar to Solove's demand for the reconsideration of public records regulations due to the emergence of new technologies, we see an urgent need for a broader reconsideration of data collection and usage practices in the US, especially with the continued development and integration of AIDC technologies. The data situation is already dire (as our examples suggest) and in danger of getting much worse. AIDC does not create a bad situation, but aggravates one that is without sufficient controls (technological or governmental) and without satisfactory public understanding to allow for just implementation. In the specific examples cited in this paper, there are always individuals who lose, but it is our belief that society takes the biggest hit as AIDC transforms individual behaviours, social interactions and class relations. An in-depth discussion of the social consequences of AIDC is beyond the scope of this paper, but we would like to underscore a few points and specifically consider AIDC's role in intensifying consumer profiling and creating fear or a sense of permanent guilt.

Consumer profiling is the recording and classification of behaviour through aggregating data. Consumer profiling is related to demographics, but it targets an individual based on specific, non-anonymous data that is sometimes bundled with more general information such as 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 at checkout. While this type of mail or coupon may be useful in some cases 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 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 loyalty cards produce nothing but savings. A common reaction from people when they hear others refuse to participate is “Well, what do you have to hide?” Most of us don’t have anything to hide, but you never know anymore. As was the case of a man who, while shopping at Von’s grocery store, slipped and fell on some spilled yogurt. When he tried to sue the store to recover for lost wages, pain, and suffering, Von’s threatened to use information from his loyalty card records against him in court. The store claimed 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 Von’s 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 — even when the data is fairly innocuous — is always a distinct possibility.



There are many times, of course, when the data is not innocuous, but very sensitive. This was the case in *Doe vs. 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”.²⁴

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 information ending up in the wrong hands. If AIDC technologies are utilized to administer health benefits (as is the case in Canada and has been proposed in the U.S.), no trustworthy systems are in place to handle the flow of sensitive information. In the U.S. personal medical information is, in fact, so unprotected that businesses such as the Medical Marketing Service exist whose sole purpose is to sell lists of persons suffering

from various ailments. To employ any technology that would further ease the distribution of sensitive medical information in the U.S., considering the country's track record, would be unwise until more safeguards are built into the health and judicial systems.²⁵

One place all Americans are now used to being treated with suspicion until they provide an ID, answer some questions, and get frisked, is the airport. After the hijackings on 9-11, airport security in the U.S. has been reviewed and tightened. Some of these changes make sense like including the prohibition against a person boarding a flight with a small knife or box cutters. 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) meaning passenger information is verified against external databases to determine that a person is who he says he is (identity verification) and to assign him a terrorist risk level (assessment). In this system passengers are required, when making a flight reservation, to provide identifying information such as name and address, a passport, Social Security and frequent flyer numbers. These details are then cross-referenced with information provided by private data firms. The end result: each traveller receives a Threat Assessment Color. In this system, green means fly freely, yellow means extra security checks, and red means not allowed on board. TSA is pressing to implement this program on all commercial flights originating in the US by summer 2004 and has supposedly been testing the program on select Delta Airlines flights since spring 2003.

One obvious problem with this plan is the government reliance on private firms to provide the essential data for identification and threat assessment. As we have seen with these companies (and ChoicePoint has been named as a potential participant in CAPPS II), they do not promise the information they provide is accurate and verification of second-, or third- or fourth-hand information becomes a game of 'pass the buck'. Other data sources for CAPPS II, such as financial and transactional records, have been named by the TSA, but there has never been any mention of the methodologies used to analyze this data to make these 'terrorist assessments'. Who is programming the computer to spot the terrorists and what rules are they following? Furthermore, there has never been any indication of how someone could inquire about an assessment, let alone contest a decision once it is made by the system. If the government is controlling who can move freely based on an automated decision-making system, the rules of the system cannot be a secret reserved for the government and its private corporate allies.

The CAPPS II system, as it has been described by the TSA, is full of inadequacies that must be addressed, reconsidered, and made transparent to those forced to abide by its rules (all citizens who fly). To our knowledge, AIDC technologies are not required for passenger check-in, as of now, but airline agents must see each passenger's driver's licence before boarding a plane.²⁶ If a passenger chooses automatic e-check-in, an AIDC technology (credit card with magnetic strip) provides this convenience. It is, therefore, not a far

stretch of the imagination to connect a system like CAPPs II with an AIDC automated check-in procedure to produce increased efficiency and provide what would be touted as 'maximum security'.

Complex Situations, Simple Solutions

So far we have attempted to give an overview of AIDC technologies and draw attention to some of its 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, workshop, and website — has been our participatory response to the various controversies affiliated with driver's licence swiping and data collection.

The Swipe project is primarily educational in that it informs people of a practice and offers an opportunity for public discussion. The performance centres on an alcohol-serving bar from which a person gets a drink and an unusual printed receipt. The receipt is all information we 'swiped' from his driver's licence at point of sale plus any additional personal information we could glean off the Internet and archived databases while the customer's drink is prepared. The workshop is a demonstration that demystifies the data collection and data warehouse businesses, offering a behind-the-scenes look at the Swipe bar. The website will be a bit different: it is a set of hands-on tools for the motivated cultural activist. On the website, you will be able to decode the 2D barcode on your driver's licence through a downloadable program, determine the value of your personal information on the open market using a data calculator, and request your own data file from the big data warehouses such as ChoicePoint. There will be a bulletin board system so people can post how many errors appear in their requested files and keep track of the response time of the data warehouses to correction requests. (Website launch date is February 2004.)²⁷

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 reason for government and industry to change practices. Resistance on the micro or individual level is also helpful. Some common strategies are paying with cash instead of using the EZ-Pass 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 barcode on drivers' licences 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 a person's information is not swiped without notification or consent. These stickers can create an interesting situation when a shopkeeper, police officer, or bouncer notices the sticker and has a moment of recognition (verbal or non-verbal) 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 Sweeny'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 and Sweeny com-

ments: "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".²⁸

These contracts, operating procedures, and laws Sweeny mentions should be considered and developed along with emerging technologies. The privacy policies in the US have been written in response to failures in a system and work as patches to immediate problems. These fixes are never complete and are often too easy to work around or totally ignore. 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. At this time we believe the implementation of AIDC technologies is irresponsible and often dehumanizing business.

We have seen that AIDC technologies are economically attractive. They reduce labour 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 behaviour to predetermined demographic cluster groups, medical conditions, and 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. Please refer to paragraph 5 of *AIDC Industry and Technologies: A Technical Overview* for further explanation.
2. Wiederer, Dan. "Answering Age - Old Questions", excerpt from *Tobacco Retailer*, June 2002, (November, 2003). <http://www.cougarmtn.com/news/featureArticle/tobaccoRetailer_Jun02.asp>.
3. Retail bar code systems are easily fooled by covering the true product bar code with one from another product. Re-Code, an interesting project by activist collective "Hacktivist" has been developed to address exactly this issue. More information can be found at <<http://www.re-code.com/>>.
4. According to a press release by Texas Instruments (TI), a manufacturer of RFID systems, prisoners at the Pima County Jail in Tucson, Arizona, will soon be monitored using RFID wristbands sold by Precision Dynamics Corporation. Livestock, wild animals, and pets have for several years been identified using implanted RFID devices (glass-coated tubes approximately the size of a grain of rice) that are injected into the body. The implanted devices are manufactured by TI and by a company called Applied Digital, which has also recently created "Digital Angel", a wearable product that tracks the health status and location of people, targeted at wandering Alzheimer's disease patients and children. The Enterprise Charter School in Buffalo, New York, has begun to experiment with RFID tracking of students with wearable badges to monitor school attendance.

5. For a reference table issued by the AAMVA please see
<<http://www.aamva.org/standards/stdUSLicenseTech.asp>>.
6. AAMVA press release, "AAMVA helps secure a safer America", 14 January 2002 (30 November 2003).
<<http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp>>.
7. The bill summary and more information about the Driver's licence modernization act can be found here:
<<http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.04633:>>.
8. Welsh, William. "Driver's licence bills: reduce speed ahead," 23 August 2002 (30 November, 2003).
<http://www.washingtontechnology.com/news/17_13/statelocal/18969-1.html>.
9. DI-tech homepage: <<http://www.idi-tech.com/manual/index.html>>.
10. Dandurant, Karen. "License scanning, now illegal, 3 May 2002 (30 November, 2003).
<<http://www.sea.coastonline.com/2002news/exeter/05032002/news/2731.htm>>.
11. Beard, Erik. "Buying Trouble: Your grocery list could spark a terror probe", 24 July, 2002 (30 November, 2003). <<http://www.villagevoice.com/issues/0230/beard.php>>.
12. Berry, William. "Cops use ID info in criminal cases", 9 April, 2003 (30 November, 2003).
<<http://www.collegian.psu.edu/archive/2003/04/04-09-03tdc/04-09-03dnews-08.asp>>.
13. Lee, Jennifer. "Welcome to the Database Lounge", 21 March, 2002 (30 November, 2003).
<<http://www.we-swipe.us/nytimes.html>>.
14. Pircg's survey: <<http://www.pircg.org/reports/consumer/mistakes/page3.htm>>.
15. Choicepoint Privacy FAQs: < http://www.autotrackxp.com/privacy_faqs.htm#correct>.
16. Epic news. <<http://www.privacy.org/digest/epic-digest05.15.01.html>>.
17. Lyon, David. *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994), p. 78.
18. One of the author's friends 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 EZ-Pass for his work commute — a drive he began to make a daily basis. Within weeks of his move, his car insurance company sent him a notice 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 EZ-Pass data the company routinely acquires. EZ-Pass FAQs:
<<http://www.ezpass.com/static/faq/speed.shtml - penalties>>
19. "Betraying One's Passengers", *The New York Times*, 23 September, 2003, (30 November, 2003).
<<http://www.nytimes.com/2003/09/23/opinion/23TUE2.html?ei=1&en=9a3c8df287b89fe0&ex=1065342076&pagewanted=print&position=->>>.
20. Electronic Frontier Foundation, "The EFF analysis of the provisions of the USA Patriot Act that relate to online activities", 27 October, 2003, (30 November, 2003).
<http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php>.
21. Gregory Palast is a journalist who extensively investigated this incident. Palast, Gregory. "Florida's flawed 'Voter-Cleansing' program", 4 December, 2002, (30 November, 2003).
<http://archive.salon.com/politics/feature/2000/12/04/voter_file/print.html>.
22. Solove, Daniel. "Access and Aggregation: Public Records, Privacy and the Constituion", *Minnesota Law Review* 86 (2002) p. 1140.
23. Ibid.
24. Solove, Daniel. "Privacy and Power: Computer Databases and Metaphors for Information Privacy", *Stanford Law Review* 53 (2001) p. 1438.

25. To read more about medical data and privacy issues in the US, see Latanya Sweeny's research at <http://privacy.cs.cmu.edu>.
26. John Gilmore is currently challenging the legality of requiring ID for air travel. See information online at <http://cryptome.org/freetotravel.htm>.
27. Please see <http://www.we-swipe.us/> for full project description and documentation.
28. Sweeny, Latanya. "Privacy and Confidentiality, in particular, computational disclosure control". <http://privacy.cs.cmu.edu/people/sweeney/confidentiality.html>.

