

Identification in the twenty-first century: The role of smart cards in the surveillance
of society and the digitization of identity management

Catherine Hawley
Professor John Turner
Communications 262
Fall 2010

“Sun Microsystems CEO Scott McNealy famously admonished the public several years ago, ‘You have no privacy, get over it’—and the public seems inclined to heed his advice” (Andrejevic, 2005, p. 109).

Part I: Introduction

The idea of surveillance is by no means a contemporary one, but the nature of surveillance in the twenty first century is changing—for better or for worse. In his book *Surveillance Studies: An Overview*, author David Lyon defines surveillance as “the focused, systematic and routine attention to personal details for the purpose of influence, management, protection or direction” (2007, p. 14). Surveillance technology keeps tabs on every aspect of our lives on a daily basis, despite our frequent failure to realize that such activity is occurring both ubiquitously and continually around us in the twenty-first century. Today’s surveillance techniques are not necessarily physically threatening or blatantly obvious. In fact, the face of surveillance is, in many cases, inscrutable. We are kept track of by the cards we swipe in the checkout line, by the tags in the clothes on our backs, and by the numerous forms of ID that reside in our wallets; all of which bring to question one of the most significant forms of surveillance, and perhaps one of the most controversial: the smart card.

The smart cards used today encompass any card with “a capability to relate information to a particular application such as magnetic stripe, optical, memory, and microprocessor cards” (General Services Administration, 2010, p. 1). Many “look like standard plastic cards, but are equipped with an embedded Integrated Circuit (IC) chip” (General Services Administration, p. 1) which helps to “store information,

carry out local processing on the data stored, and perform complex calculations” (p. 1). The “basic technology” (Livermore, para. 26) behind smart cards was introduced in the 1970s, which led to their first commercial use in 1980 by means of “pre-paid memory smart cards and smart card payphones” (Livermore, para. 26). According to Christine Blank, the smart card completed its “first major test at the 1996 Summer Olympics in Atlanta” (Blank, 1998, para. 2). The use of smart cards has been on the rise ever since; and the purpose of such technology has, and will likely continue to, come into question on behalf of not only the experts, but also the public in regards to the cards’ role in the surveillance of citizens and in the digitization and management of identity.

Smart cards have numerous and varied functions in society today, from applications in consumerism and banking to transportation and government; they are forms of identification, attached to the names and addresses of people across the globe, storing information connected to electronic databases about when, where, and how particular cards are employed by their users. These various functions, especially in the way that they contribute to the rising digitization of identification in the United States of America, each play a part in broader, more significant concepts—concepts including surveillance as a means of perpetuating what David Garland refers to as a “‘culture of control’” (Lyon, 2007, p. 12) as well as Oscar Gandy’s theory of “social sorting,” or, as Lyon defines it, the “processes of selection, inclusion and exclusion [which are] central to the operation of contemporary surveillance” (Lyon, p. 204). In addition, and as smart cards make evident, “IT [information technology] enables what current politics prescribes, the classification

and categorization of populations within regimes of risk management, in order that people from different groups may be treated differentially” (p. 204).

The idea of smart cards as a means of potential control and discrimination poses the question as to whether or not the proposed purposes of current and future smart cards are ethically sound. In looking at three separate manifestations of smart card technology, the loyalty card, the RFID tag, and the identification card, it becomes clear that each “may just be a desire for greater efficiency and marketing” (Lyon, 2007, p. 45); but also leads to some form of Oscar Gandy’s concept of “ ‘social sorting’ ” (Bennett & Lyon, 2008, p. 9), and to “ a ‘culture of control’ ” (Lyon, 2007, p. 12) in which there exists “Perennial and universal desires for security, orderliness, risk management and the taming of chance” (Lyon, p. 12).

Part II: Loyalty cards

“Loyalty cards in the supermarket...
are a key means of tracking purchases
in a way that connects back to the individual,
but numerous other means are also
used to profile and classify consumers”
(Lyon, 2007, p. 13).

Loyalty cards help consumers save money in the checkout line, but what exactly occurs when a person swipes such a card through a scanner? According to Jason Pridmore, “loyalty marketing is about rewarding those customers who frequently make purchases at a particular establishment” (2010, p. 296) as well as the “desire for personal information about consumers”(Pridmore, p. 297), which, as Pridmore points out, “likewise comes in tandem with an increased availability of

consumer data, provided by numerous third-party corporations that sell this information as a commodity and by public distributors of relevant population data” (p. 297).

In the United Kingdom, a leading supermarket, Tesco, has a database full of consumer information primarily because of customers’ usage of the company’s “Clubcard” (Simms, 2007, para. 5). This particular loyalty card, like many in the United States, helps the company “keep a record of each holder’s name, age, address, telephone number, and email” (Simms, para. 7), proving that loyalty cards are not only *smart*, but are also a form of identification.

More significantly, however, is the fact that these smart cards help companies know when, where, and what consumers are purchasing, which enables corporations to “typecast [their] customers” (para. 9). Companies can then separate their customers into various categories based on a number of characteristics, including socioeconomic status. With that information, Tesco and similar corporations can evaluate consumers and determine “how much they are worth to them” (para. 9); thus presenting the opportunity for such corporations (as well as the government) to feasibly offer as well as *bar* certain products to and from certain consumers. As Lyon points out, “Once we are identified as particular kinds of customers, it can sometimes be difficult for us to make purchases outside our box” (Lyon, 2007, p. 13).

A close friend of mine who shops for her groceries, toiletries, and other basic items at a large supermarket in New Jersey has experienced, to some degree, exactly what Lyon describes. When she picks up her receipt at the checkout line, the

database connecting her loyalty card to the store has also printed coupons for discounts on various items. The items covered by the coupons are not only specific to the items she typically purchases at the store, but are also in line with how often she buys those particular products. For example, as my friend got into the pattern of buying a certain brand of shampoo each month, the database took note of the timing of her shampoo purchases and has thus begun printing coupons for discounts on that very brand of shampoo, not coincidentally, when she is about to run out of it. If, however, she wanted to switch shampoos and try a new brand, she would not get a discount on the new product until the database picked up on her new purchasing patterns.

This may seem simple and innocent enough, but the database knows more about her than just her shampoo preferences. Based on her tampon purchasing history, the database that keeps track of her loyalty card usage practically knows her menstrual cycle, and offers her discounts on tampons on a monthly basis. On the one hand, my friend is given coupons for discounts on items that she does, in fact, want to purchase. On the other hand, though, the database has, in some sense, made her controllable; it *knows* her better than she even knows herself; reminding her of products she is about to run out, and therefore (as the company may argue) *needs* to buy again. Her situation exemplifies part of the controversy over privacy rights of consumers surrounding loyalty cards, as well as other smart cards, and is one that many people face on this and much larger, more complex scales in the twenty-first century.

Another clear model of Lyon's point is visible in the changes made to the US government's food stamp system, also referred to as the Supplemental Nutrition Assistance Program (SNAP). This program is an illustrative example of how smart cards have the potential for both positive and negative implications. For years, if a person who was on the food stamp program went to a retailer to buy groceries, he or she was required to show the cashier paper documentation, or "food coupons" (Chan, 2010, p. 31) in order to successfully buy his or her items with government aid. This method not only took up more time in the checkout line, but also made apparent who was using food stamps to other consumers waiting in line. According to the Food Research and Action Center:

Through the electronic benefit transfer systems (EBT) the use of food stamp "coupons" is no longer the means in which a client receives their benefits. EBT replaces paper coupons through use of a benefits card, similar to a bank card. USDA [United States Department of Agriculture] reports that all 50 states, DC, and Puerto Rico are now using EBT systems. (Food Research and Action Center)

With the development and utilization of the smart card, the SNAP program has been revolutionized for both its creators and its users.

Now, thanks to the new smart card EBT system, when a person on food stamps goes to a grocery store to buy food and other products, he or she uses an issued smart card to complete the purchase. In Illinois, for example, the card is called a Link card; and as the state's website describing the program explains, "Anyone approved to receive cash assistance or SNAP (Food Stamps) benefits will

be issued an Illinois Link card. The Illinois Link card is a plastic card that looks and works like a debit card. If you are eligible for cash and SNAP benefits, you will access both with the same card” (Illinois). The SNAP smart cards look just as a normal credit or debit card does, thus providing its users with privacy from other customers knowing their financial situations, as well as a speedy check-out process; saving them both the time and the embarrassment that the previous paper food stamp system often caused.

On a more Orwellian note, however, the new system has also given the government, as have many smart cards for various corporations, a much more in-depth, efficient, and easily accessible look at what food stamp receivers are buying; permitting the government to potentially begin blocking food stamp users from certain products. For example, in New York, “Mayor Michael Bloomberg has petitioned the US Department of Agriculture to add sugary beverages like soda and sports drinks to the list of things food stamps cannot be used to buy, including alcohol, toiletries, and cigarettes” (Haq, 2010, para 3). The question must be asked: at what point does having a list of items that cannot be purchased by people receiving benefits from SNAP progress from simple management and reasonable government restriction to a rather palpable discrimination against people of a lower socioeconomic status?

Loyalty cards are not the only smart card technology used by retailers today; in fact, tabs are kept on actual merchandise in the case of the next manifestation of smart cards explored in this study. And some of the very intentions—as well as

implications—that the utilization of loyalty cards present are also visible in this next type of surveillance.

Part III: RFID tags

“The goal is to encourage the loyalty of shoppers who contribute to the profit margins while discouraging those who don’t. After all, stores justify, why have unprofitable customers cluttering the store and breathing their air?”
(Albrecht & McIntyre, 2005, p. 4).

Using similar techniques and smart technology to those utilized by corporations who issue various types of loyalty cards to their customers, retail stores also have the ability to make particular predictions about each and every customer who purchases products at their cash registers—or even walks through their front doors. Many of the products sold in the United States today are each stamped with an RFID (radio frequency identification) tag containing “a tiny silicon computer chip that contains a unique identification number. This chip is often referred to as an “integrated circuit”” (Albrecht & McIntyre, 2005, pp. 13-14); the tags also contain “an antenna that’s hooked up to the miniature chip” (Albrecht & McIntyre, p. 14). RFID tags use “electromagnetic energy in the form of radio waves to communicate information at a distance” (2005, p. 13) and “are being miniaturized to the point that they can be incorporated into clothing without being noticeable to consumers” (Andrejevic, 2004, p. 9).

Not only can these tags be read by scanners in the stores at which the clothes will, in theory, be purchased; but many of them can “be tracked even after

purchase—as long as the RFID tag remains “live,” it remains readable by the scanners that will presumably be placed in stores and shopping malls” (Andrejevic, p. 10), suggesting that this particular type of smart card, too, is not as innocent at it may seem; and, in fact, takes part in far more than just helping to increase the security and manageability of merchandise.

RFID tags are a clear example of how smart technology contributes to David Garland’s theory of the culture of control. In his book *The Culture of Control: Crime and Social Order in Contemporary Society*, Garland elaborates on the “institutionalized culture of crime control” (Garland, 2001, p. xii) and various information on, as well as repercussions of, such a society stating “that criminal justice institutions have altered their emphases and the field of crime control has expanded in new directions, as state agencies and civil society have adapted to the growth of crime and insecurity that accomplished the coming of late modernity” (Garland, p. 173). Garland’s statement, although it may also (and *should*) be applied to society on a larger scale than that of consumerism and retail stores, is unmistakably visible in looking at the application of RFID tags in that such tags are an obvious example of how our society has, just as Garland says, “adapted to the growth of crime and insecurity” (p. 173) in the twenty first century. But what is the tradeoff, what other complications arise when such smart technology is used in this manner?

The way in which information is readable off of a plastic chip inside of an article of clothing or off of a product in a retail store helps companies not only keep track of inventories, prevent shoplifting, and generally increase the security and

management of that retail store or corporation, but also provides the technology for certain individuals to be, in effect, controlled by whomever reads or analyzes that information. RFID tags are a tangible demonstration of “how this new culture of control meshes with the social and economic policies that have come to characterize contemporary Britain and America” (Garland, 2001, p. xi). Furthermore, as many of the tags used in retail locations today remain readable even after purchase, the opportunity is presented not only for those tags to be scanned again in the future, but also for subsequent social sorting.

If RFID tags remain live in our clothes and readable by other RFID tag scanners in various locations including other retailers, the information about how much we have spent on our clothes in the past may plausibly morph into corporations’ assumptions about how much we will be willing to spend on our clothing in the future. By simply stepping foot into a location containing an RFID reader, we are subject to stores themselves *knowing* us, “along with, perhaps, the products on the shelves and, of course, the cash register” (Andrejevic, 2004, p. 10). This usage of smart technology walks a fine line between surveillance methods being used to increase the mere predictability of individuals and the technology being used to make deliberate assumptions, which may or may not be true, about individuals including their financial and social habits that may, as Gandy, Lyon, and Albrecht and McIntyre have reiterated, influence the way particular people will be treated. RFID technology “will allow [retailers] to assess [customers’] worth as [they] pick up products and flash [them] a corresponding customer-specific price. Prime customers might pay three dollars for a staple like peanut butter while

“bargain shoppers” or the economically challenged could be charged twice as much” (Albrecht & McIntyre, p. 4). It must also be mentioned that these types of technological advancements, whether beneficial or detrimental to society, appear far more likely to prosper and flourish in the coming years than they are to fade away and diminish. Kathryn Albrecht and Liz McIntyre predict:

In a future world laced with RFID spy chips, cards in your wallet could “squeal” on you as you enter malls, retail outlets, and grocery stores, announcing your presence and value to businesses. Reader devices hidden in the doors, walls, displays, and floors could frisk the RFID chips in your clothes and other items on your person to determine your age, sex, and preferences. (p. 3)

This proposed future of RFID tags demonstrates, just as the purpose of loyalty cards did, the issue of whether or not it is ethical for smart cards to be used as a form of not only identification, but also categorization and control. Such a future illuminates the issue of how, and if, the outcomes of certain smart cards and smart technologies live up to their original intentions, as well as sheds light on the potential for this technology to be used by larger, more powerful institutions.

Part IV: The disposition of identity and general ID cards

“Identity cards are not just technologies;
they are also contemporary tools of governance
which may be used to address a multiple
and shifting set of social and political problems”
(Bennett and Lyon, 2008, p. xi).

As daunting as the use of smart cards regarding their roles in loyalty cards and RFID tags may be, perhaps it is even more unsettling that this same technology has a function in the way large, private corporations, as well as governments, keep track of not only consumers and mall-goers, but of every citizen in a number of places. It is increasingly obvious that, in the United States and numerous other countries, citizens' identities have, in effect, been reduced, as both loyalty cards and RFID tags illustrate, to mere numbers and letters, categories and subgroups, barcodes and symbols that exist in an attempt to create “‘official identities’” (Gates, 2008, p. 221). Problems have continued to rise since even early attempts by states to “address the problem of identification” (Gates, p. 222); but, as Gates astutely points out, “At the heart of these problems is the fundamentally unstable and mediated nature of identity” (p. 222).

In an effort to combat the insecure character of identity, both private corporations and governments around the world have implemented, in many instances, various forms of general ID cards to better be able to validate the identities of certain individuals because “the verification of official identity helps to establish a relationship of trust between individuals and the institutions with which they interact with in their daily lives” (p. 220). Such cards are attached to more than

just a person's name, address, and his or her consumer tendencies. These cards represent real, live, human beings, and attempt to capture as much information about them as possible. The question is whether or not the cards and their taking part in this act of "governing by identity" (Amoore, 2008, p. 23) are doing so effectively and ethically.

One of the most common places to find the use of ID cards is on college campuses, which "have pioneered myriad uses of smart cards and keyless access systems" (Zalud, 2010, p. 56). Such cards grant students access to different buildings, particular rooms, the use of laundry facilities, access to dining halls and meals, and more. There are various types of ID cards, equipped with varying levels of security technology from the "magnetic stripe, proximity and contact smart chips" (Zalud, p. 56) to more complex and highly securitized cards. ID cards like these, no matter how basic, only further prove Lyon's statement:

Today, we are governed by identity. In a so-called information era, identification has become even more important than it was in the world of paper-based bureaucracy. The electronic information infrastructures that permit the processing of our personal data depend on identification documents and protocols to mediate between individuals and the organizations with which we relate. (Lyon, 2008, p. 500)

The more advanced, more complicated identity cards (in comparison to the basic forms previously mentioned) that exist today are generally used on a much larger scale than that of a small organization or university. These complex cards, some of which are complete with biometric technologies "that permit the measurement and

analysis of human body characteristics” (Lyon, 2008, p. 501) including “fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, each of which may be used for authentication purposes” (p. 501) appear likely to gain increasing popularity and usage during the coming years in the form of various types of ID cards put to use by both large, powerful private entities and, perhaps most importantly, governments across the globe.

Part V: National identification

“The fact is, a voluntary national ID will eventually be a reality. Americans, exhausted by long lines at airports, bridges and tunnels and frustrated with having to carry myriad forms of identification, from credit cards to passports, will eventually demand it” (Fixmer, 2001, p. 48).

Passports, drivers’ licenses, and other smart cards used by the US and state governments are utilized in the same manner that RFID tags, loyalty cards, and basic ID cards are used by private companies: to increase levels of safety, efficiency, manageability, and control, as well as “risk management and future-proofing” (Amoore, 2008, p. 25). Countries around the world have implemented different forms of national ID cards to their citizens for these same purposes—they are “new forms of identity management (IDM) [which are] being managed and used in addition to, and increasingly to replace, traditional forms of personal identification and authentication” (Lips, Taylor, & Morgan, 2009, p. 716). Such IDM systems and various national ID cards have, in the eyes of some, a darker side; their ability to contribute to social sorting and the culture of control, as well as to present

numerous other implications and complications in their usage—especially when on large (as in national or universal) scales—can be disconcerting. The controversies surrounding these new modes of managing identity make clear that “IDM moves from a narrow technical perspective to one focused upon the privacy rights of individuals” (Lips, Taylor, & Morgan, p. 718).

A number of countries around the world have already employed a national ID, and the United States began to follow suite with the development and passing of “the ‘Real ID Act of 2005’” (Gates, 2008, p. 218). The act was not well accepted by all people, and was construed by some critics as “a means of circumventing widespread political opposition to a national ID in the USA, by transforming DMV [Department of Motor Vehicles] offices into national identification registration centres and transforming state driver’s licenses into *de facto* national ID cards” (Gates, p. 218). The Real ID Act and similar developments in other countries “point to an intensification of the problem of identification in the present historical context” (p. 222)—a problem that the US Real ID Act tried to combat with the “‘securitization of identity’, especially in terms of developing more rigorous procedures to ensure that individuals ‘are who they claim to be’” (p. 226).

The question remains, however, “whether the policy would essentially create a national identification in the USA, and whether that is a desired outcome for democratic government” (p. 230). Regardless, the government, private organizations, and the public should all be aware that “Discriminatory sorting of citizens would occur [with the implementation of some new surveillance techniques like the national ID] depending on the values embedded in the specific computer

codes used to process and classify citizens' personal data" (Lips, Taylor, & Morgan, 2009, p. 718). The Real ID Act, as advocates of the act argue, "would not *require* citizens to carry a Real ID" (Gates, 2008, p. 230). But Bennett and Lyon incisively explain:

What is presented as a 'voluntary' system may in practice be hard for an individual citizen to live without. If cards are 'voluntary' (and especially if there is a charge levied), it is not hard to predict the types of people who would be unlikely to cope with the complex administrative procedures to take-up the voluntary offer: the old, the unemployed, the mentally ill, and so on. (2008, p. 9)

In addition, such an ID card system, as with the other types of smart cards described in this study, would reinforce Gates' theory that "individual identity would remain a mediated construct, an object that does not exist *a priori* but is produced in the act of documenting it" (Gates, 2008, p. 231)—in other words, the Real ID may very well produce the identities of people, rather than simply exhibit individuals' identities as those individuals see and understand them. As Gates states in the conclusion of her analysis, "No amount of technological development can transform national identity from a mediated process to an already accomplished fact. Unfortunately, this will not stop the ID enthusiasts from trying. They are convinced that the security of the nation is in the cards" (Gates, p. 231).

The question of whether countries like the United States should or should not implement a national ID in the first place elicits "a whole administrative and technological regime, and hence a complicated series of social and policy choices"

(Bennett & Lyon, 2008, p. 3). As Bennett and Lyon elaborate in their book, the question has more to do with “a range of political, administrative and technical questions [which] require careful analysis and debate” (p. 3). A national ID, just as (and perhaps more so than) loyalty cards, RFID tags, and identification cards do, would not exist as solely another smart card.

This smart card would be the “overt manifestation of [a] complex system of identity control and management” (p. 4) and would feed the same perpetuation of Garland’s “‘culture of control’” (Lyon, 2007, p. 12). Furthermore, if such cards become necessary for citizenship, “then they may be used to single out or even to harass visible minorities and those with alternative lifestyles. Thus, identity cards like college IDs, drivers’ licenses, and some national IDs contribute to the process of surveillance as ‘social sorting’” (Bennett & Lyon, p. 9). As Lyon states in *Surveillance, Privacy, and the Globalization of Personal Information*:

Such “smart” ID card systems are thus different in several respects from earlier manual and paper file systems. Among other things, they facilitate social sorting, the profiling and categorizing of populations in ways that were not previously possible and with consequences that are at present largely unknown . . . They thus have consequences for citizenship as conventionally conceived, for they promise to alter in significant ways the relation between the ‘state’ and the ‘citizen.’ (Lyon, 2010, p. 236)

Part VII: Conclusion

“Surveillance studies is in part a concerted attempt to trace some of the extraterritorial power relations of the present, visible in all manner of devices and systems, from cell phones to Web 2.0, from security cameras to biometric passports, and from credit cards to national ID cards” (Lyon, 2010, p. 1).

The manifestations of smart card technology explored in this study not only demonstrate the ways in which we are watched or *surveilled* in society today, but also show the ways in which smart cards are a means of surveillance that contributes to the digitization of identity and its various implications in the twenty-first century. More and more, we are not solely watched but are targeted and tracked in an attempt on behalf of both private organizations and governments to manage and control the population. As Lyon points out, “Whatever the purpose of surveillance, to influence, manage, protect or direct, some kind of power relations are involved” (Lyon, 2007, p. 23). Though surveillance is not necessarily intended to be an Orwellian approach to organize or supervise the general public; loyalty cards, RFID tags, and ID cards from their most basic to their most complicated forms have proven that this *1984*-esque picture is, in some light, precisely the picture being painted in the United States and other countries across the globe.

Despite the ostensible purposes of the various smart cards available and often practically forced upon us, including increased manageability, security, and efficiency, their outcomes point to various overriding themes, which are exemplified in the manifestations of smart cards explored in this study. These themes, or principles, include the way smart cards support David Garland’s “ ‘culture of

control” (Lyon, 2007, p. 12), the way they attempt to increase “risk management and future-proofing” (Amoore, 2008, p. 25), as well as the way they disseminate Oscar Gandy’s concept of “the process of surveillance as ‘social sorting’” (Bennett & Lyon, 2008, p. 9). Loyalty cards, RFID tags, general ID cards used by various government and private entities, and the proposition of implementing a national ID in the United States demonstrate Lyon’s astute realization that “Surveillance is always bound up with questions of power and its distribution” (Lyon, 2007, p. 20).

These smart technologies, from their applications in the world of consumerism to government, do, in fact, involve a question of ethics, but the matter is not so simple; one must also recognize the significance of investigating the political, economic, and social repercussions of smart cards and technologies that categorize and reduce us to mere codes and numbers; as well as compare those subsequent implications with the initial intentions behind smart card technology. In a country, and world, in which we have to continually prove our identities to governments and corporations who, more so now than ever, seem to constantly scrutinize those very identities as we claim them to be, “Telling your story no longer suffices. It is displaying your card [for better or worse] that counts” (Lyon, 2008, p. 500). This budding reality is only made more evident in looking into the way these smart technologies, from loyalty cards, to RFID tags, to ID cards of all types, have become “instruments of power, which might discriminate, infringe civil liberties and contribute to the spread of surveillance” (Bennett & Lyon, 2008, p. xii).

References

- Albrecht, K., and L. McIntyre. (2005) *Spychips: How Major Corporations and Government Plan to Track Your Every Move*. Nashville, TN: Nelson Current (Nelson Communications Inc.).
- Amoore, L. (2008). Governing by identity. In Bennett, C. J., & Lyon, D. (Eds.), *Playing the identity card: Surveillance, security, & identification in global perspective*. (pp. 21-36). New York, NY: Routledge.
- Andrejevic, M. (2004). Nothing Comes Between Me and My CPU: Smart Clothes in the Digital Enclosure. *Conference Papers -- International Communication Association*. (1-28). Retrieved Dec. 8, 2010, from Communication & Mass Media Complete database.
- Andrejevic, M. (2005). Nothing Comes Between Me and My CPU: Smart Clothes and 'Ubiquitous' Computing. *Theory, Culture & Society*, 22(3), 101-119. Retrieved Dec. 8, 2010, from Academic Search Premier database.
- Bennett, C. J., & Lyon, D. (2008). Playing the ID card: understanding the significance of identity card systems. In Bennett, C. J., & Lyon, D. (Eds.), *Playing the identity card: Surveillance, security, & identification in global perspective*. (pp. 3-20). New York, NY: Routledge.
- Bennett, C. J., & Lyon, D. (2008). Preface and acknowledgements. In Bennett, C. J., & Lyon, D. (Eds.), *Playing the identity card: Surveillance, security, & identification in global perspective*. (pp. xi-xiii). New York, NY: Routledge.

- Blank, C. (1998). Smart cards slow to garner widespread use. *Advertising Age*, 69(49), 44-49. Retrieved Dec. 8, 2010, from Academic Search Premier database.
- Chan, S. (2010, Jan. 31). Food stamp materials bound for Smithsonian. *New York Times*, p. 31. Retrieved Dec. 2, 2010, from Lexis-Nexis database.
- Fixmer, R. (2001). Get over it: national IDs are on the way. *eWeek*, 18(49), 48. Retrieved Dec. 6, 2010, from Academic Search Premier database.
- Food Research and Action Center. (18 Oct. 2000). Retrieved Dec. 5, 2010, from (<http://frac.org/federal-foodnutrition-programs/snapfood-stamps/>).
- Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. Chicago: The University of Chicago Press.
- Gates, K. (2008). The United States Real ID Act and the securitization of identity. In Bennett, C. J., & Lyon, D. (Eds.), *Playing the identity card: Surveillance, security, & identification in global perspective*. (pp. 218-232). New York, NY: Routledge.
- General Services Administration: United States Government. (2010) *Smart card technology—a tutorial*. Retrieved Dec. 12, 2010, from http://www.idmanagement.gov/smartcard/tutorial/tutorial_text.pdf.
- Haq, H. (2010, October 26). What can't food stamps buy? New York City wants sugary drinks on 'no' list. *Christian Science Monitor*. Retrieved Dec. 5, 2010, from Academic Search Premier database.
- Illinois. Dept. of Human Services. *Illinois LINK card*. Retrieved Dec. 5, 2010, from (<http://www.dhs.state.il.us/page.aspx?item=30371>).

- Lips, A., Taylor, J., & Organ, J. (2009). Identity management, administrative sorting and citizenship in new modes of government. *Information, Communication & Society*, 12(5), 715-734. Retrieved Dec. 5, 2010, from Communication & Mass Media Complete database.
- Livermore, A. (2003, Oct. 22). The inside of a 'smart' story: smart cards are increasingly becoming relevant in our everyday life. *eworld tracks the scene. Business Line*. Retrieved Dec. 8, 2010, from Lexis-Nexis database.
- Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, 22(9), 499-508. Retrieved Dec. 4, 2010, from Academic Search Premier database.
- Lyon, D. (2010). Introduction. In Y. E. Chan, E. Smith, D. Lyon, L. Harling Stalker, & E. Zureik (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information* (pp. 1-7). Quebec: McGill-Queen's University Press.
- Lyon, D. (2010). National ID Card Systems and Social Sorting: International Public Opinion. In Y. E. Chan, E. Smith, D. Lyon, L. Harling Stalker, & E. Zureik (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information* (pp. 236-256). Quebec: McGill-Queen's University Press.
- Lyon, D., (2007). *Surveillance studies: An overview*. Malden, MA: Polity Press.
- Pridmore, J. (2010). Loyalty Ambivalence in the United States and Canada: The GDP Survey, the Focus Groups, and the Context of Those Wonderfully Intrusive Loyalty Cards. In Y. E. Chan, E. Smith, D. Lyon, L. Harling Stalker, & E. Zureik (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information* (pp. 295-309). Quebec: McGill-Queen's University Press.

Simms, A. (2007, June 25) Getting to know you. *New Statesman*. 136(4850), 24.

Retrieved Dec. 8, 2010, from MAS Ultra-School Edition database.

Zalud, B. (2010). Are smart cards a no-brainer?. *Security: Solutions for Enterprise*

Security Leaders, 47(6), 56-58. Retrieved Dec. 5, 2010, from Business Source

Premier database.

Research Strategy Essay

The composition of any research paper requires investigation, planning, and dedication to a topic—from the initial selection, to the composition of each draft, to the finishing touches on the final essay. The research preceding the composition of this particular paper involved not only the use of traditional literature from the Goucher College Athenaeum, but also the use of online databases, InterLibrary Loan services, and hours of contemplation, drafting, and subsequent revision of the essay. The result of my commitment to the research process includes a tangible paper, as well as newfound knowledge and experience regarding the research and writing process.

As soon as this paper was assigned, it was made clear that my topic would involve some aspect of surveillance. The question, henceforth, became one not of *what* but rather *what part* of the broad theme of surveillance my particular paper would focus on throughout its suggested twenty page length. Class discussions sparked my initial interest in smart cards; and through the use of online databases accessible through the Goucher College website, I was able to find a number of sources regarding smart cards and their relation to surveillance and identification. The information available on the databases further honed my research and took it in a more specific direction; thus I looked for additional information online, in print form in the Athenaeum, and through the InterLibrary Loan services.

The aforementioned techniques and resources that I employed to complete my research taught me some significant lessons about the research process regarding the time, energy, and perseverance one must apply in order to compose a

research paper. Without the use of these resources and research strategies, the research process itself would have been hindered, and the act of composing such a paper would have been delayed, if not halted entirely. My devotion to this study has resulted in a lengthy exploration of my topic, through which my research comes across, I hope, as both evident and pertinent to readers.