GOVERNANCE, SECURITY AND TECHNOLOGY: THE CASE OF BIOMETRICS

Elia Zureik with Contribution from Karen Hindle

Introduction: Governance, Government, and Governmentality Several writers have advanced "governance" as an alternative framework to the traditional notion of "government." At the state level, governance emphasizes cooperation between the civil and political spheres of society, whereas government is usually thought of in terms of the formal political structure of the nation-state—its executive and legislative branches. Governance is intended to "bring the citizen back in" by stressing participation, accountability, transparency, and human rights as basic elements in the management of society. Because of its ability to connect individuals and groups to the centres of power, information technology is being singled out as a requisite for good governance.[1] It is also being seen, however, as a double-edged sword with the potential of facilitating wider control of information and centralization in formal state structures to the detriment of good governance; state surveillance is advanced by the critics as a case in point.[2]

Governance is more encompassing in its reach because it allows us to locate power outside the formal boundaries of government. Foucault's notion of governmentality is useful in furthering our understanding of governing beyond the formal conception of the citizen and her relationship to the state. Governmentality focuses on the constitution of the self in the power nexus of society's institutions, political or otherwise. It acknowledges power in its productive aspects i.e., it reconfigures the subject but, at the same time, creates resistance. Through governmentality, the citizen is viewed as an active subject, though labouring under "complex chains of constraints, calculations of interests, patterns and habits, and obligations and fears."[3] For us, governance involves not only understanding "relations of ruling" (to quote

Dorothy Smith)[4] in their political, economic, and formal sense, but also the nature of the discursive practices used to administer and manage people through what Michel Foucault calls "bio-politics."[5] In its totality, governance involves the use of knowledge (technical, social, administrative) to manage population groups through identification, categorization (inclusion and exclusion), and a monitoring process the purpose of which is to create a disciplinary, hegemonic regime based on self-normalization.[6]

Security and Technology Security is usually defined in military terms to refer to national security. Security thus defined aims at protecting the nation-state from external threats. With an increase in religious, ethnic, and racial conflicts within states, the United Nations agencies and some countries—Canada in particular—began to view human security as a complementary concept that concerns itself with human rights, protection of the environment, and guaranteeing of basic needs related to health, education, and personal security.[7] Human security and good governance dovetailed as requisites for a stable international order. Yet, national-cum-military security remains the defining feature of security as articulated in state policies. The events of 11 September 2001 have further dashed any hope that human security will establish a lasting foothold in the security discourse and pose serious challenge to the military and technological conception of national security.

But security in its various dimensions has a longer history. High modernity, Peter Manning claims, has transformed personal security from its internal and immediate context based on communal life and interpersonal relationships to one that depends upon external factors such as technology.[8] Technology is being touted as the main tool of risk assessment and the guarantor of security. This substitution has created an illusory sense of security which, in turn, has given rise to "corrupting" influences manifest in appeals to "technological conceit:"

> Agents of control, governmental experts in security and private corporations that carry out risk management and risk estimates for business, those who promote and sell high tech devices - machines to read retinas, explosive detectors, "smart" cards that contain personal information in a chip in a card,

> and the mirage of electronic protections in and around airports and computer-based data, promotes the [corrupting] illusion. The anxious public is willing to pay for them directly and indirectly and promote the illusion. The public, eager for reassurance, accepts the efficacy of such innovations.[9]

Manning goes on to suggest that at times of crisis, such as in the aftermath of 11 September, something akin to a panic campaign is orchestrated by state agents of social control, supported by a media-simulated depiction of the enemy as a shadowy, external "other." Terrorism is no longer associated with understanding the context of action, but with singling out certain groups who are profiled on the basis of national origin, race, and religion. Surveillance becomes part of a "tautological" universe in which, to quote Gary Marx, "everything that moves" and is captured on a video camera becomes part of a deviant world.[10] To put it another way, "The claim is that what is seen can and must be controlled, rather than seeing what is seen as a limited, specialized, rather flawed narrow window into the violent complexity of humanity."[11]

Mariana Valverde makes a related point that security is an abstract concept, not something to be measured and quantified: "The impossibility of guaranteeing security is rooted in the fact that like justice, and like democracy, 'security' is not so much an empirical state of affairs but an ideal—an ideal in the name of which a vast number of procedures, gadgets, social relations, and political institutions are designed and deployed."[12] In the context of post-11 September events security, according to her, meant "state security" and not necessarily "citizen security." State security has been defined in a Hobbesian, zero-sum fashion and is monopolized by experts and professionals who by-pass public participation and design "top down" security solutions. In noting that American and Canadian antiterrorism legislations extend beyond immediate, temporary concerns to deal with immigration and other issues of personal and public nature, we end up with "governance through security."[13]

This paper addresses the nature of biometric as "body technology," with claims to authenticate identity and enhance security and trust. Both in Canada and the United States, the campaign to introduce the technology

has triggered national debates. The discussion surrounding these debates will be situated in the context of American and Canadian antiterrorism legislations introduced after 11 September 2001. Because of their claims to authenticate and verify personal identity on the basis of behavioural and physiological features, biometrics are presented as desirable key elements in the categorization and processing of people such as immigrants, travellers, welfare recipients and eventually citizens through the introduction of a biometric national identity card. As shown in the final part of the paper, this raises fears of using the technology for social profiling purposes.

Body Technology: Dimensions of Biometrics DNA "fingerprinting" and biometrics are two monitoring technologies that focus exclusively on the body as a unique identifier of individuals. While DNA analysis uses blood, body fluids, hair, and human tissues for unique identification purposes, biometrics use human physiology and certain types of behaviour such as voice recognition, gait, and signature analysis. Those who write about identity authentication and security are fond of making a distinction between something one knows (such as a password or personal identification number (PIN)), something that one has (such as a card key or smart card), and something that one is i.e., a biometric. The assumption here is that it is possible to forget, lose, or fall victim to fraud because of what one has or knows, but one will always be what one is—at least in terms of body parts.[14]

The International Biometrics Industry Association (IBIA), an advocacy organization that represents major biometric companies in the United States, defines biometrics as follows:

> Biometric technology involves the automatic identification or verification of an individual based on physiological or behavioral characteristics. Such authentication is accomplished by using computer technology in non-invasive way to match patterns of live individuals in real time against enrolled records that use face, iris, hand, fingerprint, signature, and voice measurements in applications such as border control, information security, physical access control, financial privacy safeguards, time and attendance management, law enforcement, and other civil and government uses.[15]

Biometric technology uses two main methods for identity checks: verification (sometimes called authentication) and identification. Verification confirms that people are who they say they are, while identification determines who the person is. Regardless of the biometrics measured, the technology relies on pattern recognition, which converts images into a binary code by means of an algorithm. To use the verification system, individuals must enroll first, which involves submitting an identifier such as an identity card, and then linking the information obtained from the document to biometric (hand, eye, fingertips, etc.) images. A reference template is created and stored to link information on the document to unique biometric data. This reference template must be updated to incorporate any physiological changes of the enrollee. Verification is accomplished when an individual presents an identifier with which he enrolled, and the system compares the trial template with the reference one. Verification is referred to as one-to-one matching. Identification, on the other hand, is one-to-many matching. The idea here is not to confirm that people are who they say they are, but to check if the temporary template is present in the stored files of reference templates. In other words, one's biometrics are compared against the many that are stored in the system. An example here would be a passenger whose scanned image (trial template) is compared to many existing reference templates, such as those who are on an FBI "watch list." Another example provided by the US General Accounting Office (GAO) is to check on a welfare recipient for negative matching. Here the system attempts to verify that the recipient is not "double dipping," i.e., using fraudulent documentation with multiple identities to qualify for welfare.

Biometrics as Trust Enhancing Technologies Writers on surveillance concur that underlying the need for surveillance is a lack, or potential lack, of trust by those in positions of power vis-à-vis those who are below them. This is true whether the surveilled is classified as a deviant or normal person. For our purpose, however, surveillance is examined in so-called normal situations, in everyday life, particularly in organizational settings such as airports, workplaces, and public arenas. Of the various factors mentioned in the discussion of monitoring and surveillance, risk and trust rank paramount.

Under this conception, surveillance technology is construed as a trust-enhancing tool. And the more capable the technology is of capturing people's unique biological identifiers, the more reliable and trustworthy it is perceived to be – particularly by its promoters. For this reason, genetic profiling and biometrics occupy a special place in the range of available surveillance technologies. According to David Knights, et al.:

> One response to pressures to find means of manufacturing trust has been to collect and check details of users' physical characteristics through the use of retina scans, hand geometry, fingerprints, voice recognition, digitized photographs, and DNA.[16]

Knights and his colleagues question if this technology, even when used in combination with smart cards that carry a user's biometric information, will contribute to greater (manufactured) trust and lower the risk levels among users, as its promoters claim. It is difficult to say, they conclude, because of the dialectical relationship between control (power) and agency. If trust in institutions depends on the type of technology in use, trust in technology is also a function of level of trust in institutions that use the technology to begin with. Thus, "the consuming public may express mistrust in the data collection activities of business in general, and financial institutions in particular. Yet, at the same time, it shows a willingness to 'entrust' ever increasing amounts of personal data to those same businesses and institutions in exchange for various benefits."[17] And "such methods of personal authentication constitute an uneasy mixture of strategies and activities which elude allocation along the trust/control opposition."[18] Clearly, biology as a signifier of persona is back in use, and is in the process of displacing impersonal technologies that rely on PINs and passwords. In a telling manner, the body (eyes, hand, and face) returns as the absent Other, this time encased in biometric technology. Thus, instead of the eye being the source of the surveillance gaze, now the eye becomes the object of the gaze.

A view of surveillance from the point of view of the surveilled argues that, under certain conditions, surveillance can create a criminogenic environment that encourages distrust, stigmatizes innocent people, and may victimize those affected by it.[19] In contrast to objective crime wherein the effect of

criminal behaviour is immediate and visible, surveillance-type victimization falls under the subjective crime category that is associated with psychological and emotional stress, which in certain cases can outweigh objective, material loss. McCahill and Norris cite examples of army personnel who were punished for refusing to give DNA evidence to their superiors. Other cases of surveillance victimization involve insurance companies and employers[20] who share information about their employees and clients with third parties, and in the process jeopardize a terminated employee's prospects of securing employment elsewhere.[21]

To cite another example borrowed from biometric technology, face recognition has received extensive press and media coverage as a promising and reliable surveillance tool in security-conscious environments. Yet, the reliability of face recognition technology has been questioned, and some even describe it as impractical. David Birch demonstrates the point by using the example of London Heathrow Airport, which processes in excess of one million passengers weekly.[22] For the sake of example, he assumes that 10 individuals who are the real targets of security checks pass through the screening system and are accurately identified by the cameras. With a success rate of 99.90 percent, face recognition cameras will end up registering around 990 cases of false positives (.001 of 1 million), in addition to the 10 targetted individuals. To verify and reject close to one thousand false positives per week—averaging more than one hundred cases per day—is impractical. It would surely be costly and overload the surveillance system. Birch concludes by pointing out that face recognition technology, similar to closed circuit television (CCTV), may make us "feel" safe; in reality, however, we are not any safer.

The effectiveness of face-recognition technology depends on the quality of the captured images, camera angle, and lighting. Effectiveness is also constrained by changes in the physiological features of the target. It is difficult to capture accurate images of people in motion or far away from the cameras. Changes in appearance, such as one's hairstyle, a new beard, or glasses, will also cause problems in matching captured images with information stored in databases. Face recognition is more reliable in static situations, such as in workplaces and other organizational settings where individuals are

required to submit to routine checks and provide up-to-date information on their appearance.

A recent report prepared by the US National Institute for Standards and Technology recommends the combined application of face recognition and fingerprint scanning technologies on all foreign visitors to the United States. Based on test data provided by the State Department, the study discovered 90 percent accuracy in one-to-one face recognition (the person scanned is actually the same one to whom the document was issued), and one percent false positive rate. In the case of pictures with low quality, the accuracy rate declines to 47 percent. In the case of one-to-many searches (matching a single face against a database), identification had a success rate of 77 percent. Although finger scanning accuracy rate exceeded face recognition, "fingerprint recognition had its problems as well, especially with individuals whose fingertips had worn down, like farm workers, house cleaners, and the elderly."[23]

The Electronic Privacy Information Center (EPIC), a privacy advocacy group in Washington, DC, lists six areas of concern in the use of biometrics: 1) method of data storage and whether it will be centralized or decentralized; 2) data vulnerability to theft and abuse; 3) confidence level in carrying out authentication, and the implications of errors such as false positives or false negatives; 4) knowing how to judge whether the information is authentic; 5) being clear on who decides about possible linkages of biometric information to other types of information such as police records, consumer habits, etc., and 6) any unintended consequences at the societal level of having citizens being constantly under the gaze of cameras and other video surveillance equipment.[24]

These are not exactly reassuring results from the point of view of good governance. While the state may persist in deploying the technology in the name of governmentality and the administration of people—seen for example in the current government drive in Canada and other western countries to introduce national identification cards that use biometrics—privacy violations and other social costs resulting from such an undertaking may outweigh claims of efficiency and indeed security. In particular, as shown in this

paper, such technological measures may end up stigmatizing marginal groups and visible minorities.

Promoting Biometrics: The United States In spite of expressed doubts about the efficacy of the technology, the biometrics industry persisted in promoting its role in guaranteeing security at the personal, institutional, and national levels. This became most apparent in the marketing strategy of the biometrics industry in the wake of 11 September. The economic payoff for the biometrics industry in the United States has been substantial. With a budget of $38 billion for Homeland Security Administration, major defense manufacturers are adapting their technologies for domestic use. In the words of one commentator, "11 September, created a long-waited moment for the biometric industry."[25] The 11 September attack came at a time when the high-tech and dot-com industries were in a severe economic slump, following the boom period of the 1990s. One report estimates that the size of the biometric market would exceed $4 billion in the United States in 2007, which would reflect an 80 percent growth in the market.[26]

A panic campaign that went into effect after the terrorist attacks on the twin towers of the World Trade Center in New York was seized upon by the biometrics industry to market its wares. In the words of George Radwanski, former Canadian Privacy Commissioner:

> In the days and weeks following the attacks, the general public got a good look at what privacy advocates have been worrying about. They saw that there is a huge industry eager to manufacture and sell the technology of surveillance: video cameras, facial recognition systems, fingerprint readers, e-mail and web-monitoring, "smart" identification cards, location tracking. And they saw how many people are eager to argue that if you don't have anything to hide, you shouldn't mind revealing everything.[27]

Within a fortnight of the 11 September attack, the IBIA issued a press release highlighting the role of biometrics in the fight against terrorism.[28] While the statement advised against the overly optimistic view that biometrics alone could provide the "panacea" for combating and halting terrorism, the advocacy group never doubted the scientific and technological

competency of its member companies. Any shortcomings had to do with insufficient government backing. What the industry needs is government support so that biometrics will occupy "mainstream applications for improved security."[29] In the press release, the mission statement of the IBIA stressed its role in assisting government agencies through "unobtrusive" methods to detect criminals and illegal travellers at airports and international borders, protect the national communications infrastructure, prevent unauthorized physical access to security-sensitive locations, and unauthorized virtual access to "sensitive information systems and data."

Probably the boldest statement promoting biometrics as an essential tool in the fight against terrorism comes from a white paper put out by Visionics, an American manufacturer of face recognition technology, which was recently acquired by Identix, a large manufacturer of fingerprinting technology. In *Protecting Civilization from the Faces of Terror*, the company reminded its readers that airport security, which is the responsibility of the federal government, "demands substantial financial resources" so as to develop a "technology that can be implemented to immediately spot terrorists and prevent their actions." Boarding a plane should no longer be considered "a right granted to all, but as a privilege accorded to those who can be cleared as having no terrorist or dangerous affiliation."[30] A headline in the *New York Times* described this two-tiered approach as "reverse profiling" in which, for an annual fee, travellers can enroll in the system, have their biometrics stored on a pass card for speedy processing at airports, and exercise their "class consciousness."[31] What follows from this is clear: there is a need to verify the identities of millions of people who board planes daily and "biometrics are the only means available to achieve this."[32] Biometric deployment would not be limited to national borders; it would also be used to secure "a more effective international security framework."[33] Facial recognition and finger scanning technology, which are at the heart of airport and border security, will have to work in tandem with intelligence agencies which are asked "to build databases of terrorists' faces and identities. These can be used to track them through computerized facial recognition."[34] As a matter of fact, the whole system hinges on intelligence agencies developing and maintaining "terrorist watch lists." This task has begun in earnest in the United States.

A "master terrorist watch list" containing 100,000 names has been developed by the FBI, the CIA, the Justice Department, the Department of Homeland Security, and the State Department, about which civil rights and privacy advocates have expressed serious concerns. They fear that the list will give the government wide power to store and collect information on people who have no connection with terrorism.[35]

What makes facial recognition "most suited," according to Visionics, is its ability to "function from a distance, in a crowd and in real time without subject participation."[36] Authentication, the white paper advocates, should be equally applied to airport and other transportation employees.

The same message is provided in a white paper issued by the California office of Bioscrypt, a Canadian biometric company based in Toronto. Advantages of fingerprint biometrics were outlined for both employers and employees, but they were mainly aimed at employers. For employers, biometrics are used to screen employees, access control and keep track of attendance, while for employees biometrics make it possible that "instead of having to carry around the office keys, you simply bring your finger with you."[37]

Nuance, another California biometric company that manufactures speech recognition technology used mainly in call centres, describes its product as an essential money-saving tool for business, since it costs as little as 1/12th the cost compared to using live agents to answer telephone calls.[38]

In their testimonies before the US Senate Subcommittee on Technology, Terrorism, and Government Information, the executive directors of the IBIA and the Biometrics Foundation (BF), a two-year old organization dedicated to researching and raising public awareness of biometrics, reiterated many of the above points, and stressed others such as the need to protect security of national infrastructure, individual privacy, and mount programs to educate the public about the technology.[39]

Paul Collier of the BF told the Senate Subcommittee on 12 October 2001 that the United States is ahead of other countries in developing the technology, but lags behind in implementing it. Biometrics provide increased security while, at the same time, protecting privacy. Since other countries use the technology, Collier called for "encoding biometric data in passports, visas,

identification cards, and other travel documents."[40] Echoing the words of his colleague, Richard Norton from IBIA, Collier proceeded to tell the Subcommittee on 17 October 2001 that biometric technology will act as a "digital lock and key on personal information."[41] He sounded a word of caution that the success of the technology depends on the trust of travellers and on it being used responsibly.

By late October 2001, members of the IBIA were "deluged with requests for testimony at hearings and for direct advice and counsel from staff and Members of the Congress and from senior officials of the executive Branch."[42] During the same short period of a few weeks after the attacks on New York and Washington, no fewer than nine bills were introduced in the House of Representatives and another eight in the Senate. These bills called for the implementation of biometric technology in one form or another (with special focus on fingerprint technology) in order to tighten immigration, visa, and naturalization procedures, allow tax benefits to companies that use biometrics, and check employee background at border and maritime check points. The House bills culminated in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act), which was signed into law on 26 October 2001. The Bill requires consular offices of the US government to obtain fingerprints from visa applicants in their home countries.[43]

Canada On the Canadian side, the issue of biometrics is equally salient, but the size of the sector is naturally smaller. In early January 2002, a biometric advocacy group was established within the Canadian Advanced Technology Alliance (CATA). The mandate of the CATA Biometrics Group (CBG) includes "a comprehensive public education strategy that compels industry and government to recognize the value of biometrics technologies," "protection of privacy and the integrity of personal data," "the creation of secure environments that protect both people and information," and to "empower people to choose biometrics to enable their applications … with peace of mind."[44] The executive director of CBG, Howard Stanley, spelled out in greater detail the role of biometrics in society using "computer technology in noninvasive ways [to] help us attain the security levels our soci-

ety requires, while streamlining commerce, avoiding fraud and abuse and reducing waste."[45] He went on to say that "biometrics will increase privacy, not decrease it," and that "civil rights [is] an area where policies must be advocated to ensure that freedoms are respected."[46] To demonstrate its concern for privacy, the CBG promised to coordinate with the Canadian Privacy Commissioner and Justice Canada.

While there is promise of future cooperation between the American and Canadian biometric advocacy groups, at the governmental level a close coordination is already in place. Following the 11 September 2001 attacks, Tom Ridge, Director of the US Homeland Security Administration, met on 12 December 2001 with Canada's Deputy Prime Minister John Manley to discuss means to strengthen border security between the two countries. The Standing Committee on Citizenship and Immigration issued its report *Hands Across the Border*, which included recommendations dealing with increased coordination between the United States and Canadian authorities and the use of new technologies. In response to one of the recommendations, the government of Canada agreed that "The implementation of new technological tools is essential to successful intelligence gathering activities. This includes increased use of biometric tools, electronic finger print systems, linked databases and proximity card technology."[47]

These efforts resulted in "The Smart Border Declaration" and "The 30-Point Action Plan." The latter was released on 9 September 2002 during a meeting between George W. Bush and Jean Chrétien. Included in the 30-point plan is the need to develop common standards for biometric use for iris scanning and fingerprinting which would incorporate "interoperable and compatible technology to read these biometrics" along border points between the United States and Canada.[48] As a starter, Canada undertook to introduce a new Canadian Permanent Resident card that is "biometric-ready" and to implement the NEXUS-Air pilot program for air travellers. This will be in addition to exchanging information about airline passengers between the two countries in advance of travel. Thus, Canada and the United States have agreed to share Advanced Passenger Information and Passenger Name records on high-risk travellers destined to either country. As well, the two countries will work towards developing "compatible immigration databases."[49]

Although it does not spell out what constitutes "high-risk travellers," it is becoming clear that the designation refers to people of colour, minorities, immigrants, and refugees. Gentleman argues that the introduction of biometric ID cards in Europe does not bode well for "migrant workers," and "is associated with police abuses and repression of minority groups." She continues to say that "there is evidence in continental Europe that members of ethnic minorities are asked to provide ID [cards] more often than other citizens."[50]

This particular program, called the Advance Passenger Information/Passenger Name Record (API/PNR), which will be administered on the Canadian side by the Canadian Customs and Revenue Agency, drew sharp criticism from Canada's Privacy Commissioner, who dubbed it the "Big Brother" database. In a letter dated 26 September 2002 to Elinor Caplan, the minister responsible for the program, Commissioner Radwanski stated:

> Very frankly, the government of Canada has no business systematically recording and tracking where all law-abiding Canadians travel, with whom we travel, or how often we travel. And the government of Canada has no business compiling databases of personal information about Canadians solely for having this information available to use against us if and when it becomes expedient to do so. Such behavior violates the key principles of respect for privacy rights and fair information practices, and has no place in a free society.[51]

The criticism was repeated in a letter sent to Caplan on 12 November 2002 and endorsed by six provincial Privacy Commissioners.[52] On 9 January 2003, the federal Commissioner released another letter sent to Caplan in which he cited endorsements of his position from other legal experts, such as a former Justice of the Supreme Court and a former Justice Minister of Canada.[53] Finally, on 9 April 2003, the Privacy Commissioner of Canada released a statement and an appended letter from Caplan in which she acknowledged the privacy concerns of the Commissioner, and outlined steps taken by her Ministry to insure that data collected on air travellers will be limited in scope and access to safeguard privacy.[54]

Bill C-36, 2001, the Anti-Terrorism Bill, is Canada's main response to the 11 September events. In commenting on the Bill in its draft stage, David

Schneiderman saw it as a response to living in a "risk" society.[55] Such a response, according to him, can be understood in terms of three factors: first, that the risk society is a global society in which risk transcends national borders; second, that the risk society tends to over-rely on "expert and professional knowledges," and third, that there is a tendency to "overreach" by adopting legislations which profess to cope with risk, without paying sufficient attention to rights and freedoms.[56] Lisa Austin was more emphatic in pointing out that privacy will be the biggest casualty of Bill C-36, because "[t]he anti-terrorism legislation, and other impending reforms, increases the level of surveillance in our society."[57] In its brief to the House of Commons Justice Committee, the Ottawa-based Canadian Centre for Policy Alternatives (CCPA) expanded on the list of concerns regarding Bill C-36, and pointed out that the Bill does not contain a sunset clause.[58]

The final version of the Act responded to some of the concerns voiced by the critics. For example, a sunset clause extending over five years is now included in Bill C-36, except that the clause does not cover the entire Bill, as some would prefer, but is limited to provisions dealing with preventive arrest and investigative hearings.[59] Similarly, amending the Access to Information Act, giving government the right to withhold public access to information for as long as fifteen years, provides "little comfort to those facing criminal and immigration proceedings where access to vital information has been denied on the grounds of national security."[60]

Debate in Canada over the introduction of a national ID that uses biometric data is in its infancy,[61] although it is gathering momentum. Immigration Minister Denis Coderre appeared before the House of Commons Immigration Committee to explore the need to adopt such a biometric ID in order to expedite entry-exit control to and from the United States. Coderre suggested the adoption of an offline system wherein biometric information stored on the card will not be linked at a central database, but will be checked against card holders.[62] By invoking privacy concerns, the *The Globe and Mail* editorialized against the proposal whose intention is "to satisfy the Americans."[63] Canada seems to be inching closer to adopting national ID cards, as evident in Coderre's statements when he hosted a Citizenship and Immigration Consultation Forum in Ottawa in

October 2003 to discuss the adoption of biometrics in national ID cards.[64] If the panellists are any indication, the forum was heavily weighted in favour of a national ID card. Among those featured at the forum were industry spokesmen, biometrics advocacy groups, and officials from other countries that either have adopted or are on the verge of adopting biometrics, such as the European Union and the United Kingdom. Quebec's Privacy Commissioner was the only provincial privacy representative to address the conference. Alan Dershowitz, a Harvard law professor and keynote speaker at the forum, who is also known for condoning preemptive assassinations and "mild torture" as means of self-defense by governments, provided a rationale for adopting biometrics technology. He argued that the technology does away with subjective evaluations by officials in charge of administering travel and immigration procedures.[65]

What is significant about the Canadian data is the willingness of the public to endorse the use of biometrics and ID national cards in order to check against fraud and abuse of government services. For example, 78 percent of those who condoned the introduction of biometrics ID national cards, did so in order to "reduce the abuse of government programmes," thus giving credence to the argument that the technology is on the way to becoming a surveillance tool in the arsenal of a declining welfare state.[66]

Social Profiling and Reaction to Biometrics The purpose of this section is to analyze public attitudes to biometrics and privacy in the wake of 11 September. There is a deeply ingrained attitude in western societies that equates technology with progress; anyone who is skeptical about the use of technology is liable to be portrayed as standing against progress. In the post-11 September era, to object to technology is tantamount to compromising state security. As argued by Mike Davis, "the globalization of fear became a self-fulfilling prophecy" after 11 September.[67] When portrayed as a safeguard against terrorism, identity theft, and general personal insecurity, several surveys that will be dealt with here confirm wide public acceptance of invasive biometric technology. It should be pointed out, however, that this acceptance is tempered with high levels of concern about privacy issues. This is true in the United States, Canada, and Britain.

Biometrics technology is being introduced primarily in passports and at locations such as airports and border crossings. As we have shown above, concerted efforts are being made in Canada and other Western European countries under the auspices of the European Community to introduce biometrics as a means of administering immigrant entry. A spokeswoman for the European Commission, in charge of the biometrics project, spoke at the Ottawa forum and made it explicit that the thrust of the Commission's adoption of biometrics is to check the movement of illegal immigrants and seekers of refugee asylum. The Electronic Frontier Foundation (EFF) points out immigrant and refugee groups are unlikely to object to the use of biometrics for identity checks since they lack any power to speak of and do not have an advocacy group to lobby on their behalf. The EFF also warns that the same technology could become part of creeping surveillance apparati whose uses will extend beyond borders and airports, and immigrant and foreigners. This is probably more true for the United States than it is for Canada where the impact of immigration on Canadian life is more pronounced through the presence of numerous community-based ethnic associations and lobby groups, and where multiculturalism is more entrenched in legislation and public consciousness. Clearly the use of biometric technology in the fight against terrorism has direct bearing on racial and other types of profiling—welfare recipients, for example—and indeed on governance as a whole.[68] Bill C-36 in Canada is a clear example of this. This was also the case in several post-11 September legislations in the United States. For example, in addition to the USA-Patriot Act (2001), the Enhanced Border Security and Visa Entry Reform Act (2002), the Aviation and Transportation Security Act (2001) and, previous to this, the Illegal Immigration Reform and Immigrant Responsibility Act (1996) —all of which specifically mention biometric technology. There are two other Acts which do not mention biometrics as such, but the language of the Acts lends itself to the deployment of biometrics. These are the Personal Responsibility and Work Opportunity Act (1995), aimed at welfare recipients, and the Immigration Control and Financial Responsibility Act (1996), intended to verify immigration status and eligibility for public assistance.

By using biology and physical appearance as means of identification, biometrics are likely to legitimize group differentiation and racialization in society in the name of security. The surreptitious nature of the technology and the ease with which it can be used leave little room for escaping the gaze of the authorities.

Following 11 September, several surveys were carried out in the United States concerning the use of technology for establishing identity.[69] One of the most detailed national opinion surveys focusing exclusively on biometrics was carried out in the United States in September 2001, a week after the attack, and repeated in August 2002.[70] The proportion of those exposed to biometrics is fairly small, hovering around five percent in the 2002 study and four percent a year earlier, which, when prorated for the United States population, amounts to 10 million people. Within the five percent who reported experience with the technology, a large majority (from 72 percent to 85 percent depending on the type of biometric) reported "general comfort" in using the technology. Yet close to 90 percent expressed concern about possible misuse of personal information collected through biometrics, and more than one in four (28 percent) reported personal privacy victimization. ID-based fraud was ranked by 95 percent of the sample as a serious problem, with around 20 percent saying that they have been victims of ID fraud. Biometrics is perceived by the majority of respondents as a safeguard for passport identity verification (88 percent), access to secure government buildings (84 percent), airport check-ins (82 percent), identity for driver's license (77 percent), and car rental (60 percent). Overall, around two-thirds stated that the technology should "not be misused in ways that would threaten legitimate privacy." Those with low income and education, women, and conservatives all expressed high-level confidence that biometric technology would not be used for purposes other than to detect terrorists. Between 85 to 95 percent endorsed the use of biometrics by government authorities to screen entry in high-security government facilities and schools, licensing special occupations, facilitated entry at passport control, and for people receiving welfare cheques.

What is significant about the rest of the findings is the sheer magnitude of endorsement by the public of Fair Information Practices i.e., that people

should be informed in advance about the use of the technology (95 percent), that information should not be collected secretly (95 percent), should not be used for purposes other than what it was originally collected for (95 percent), should be coded and not shared (94 percent), should not be combined with other personal identifiers (86 percent), that citizens should have the right to check if the information stored on them is accurate, and that biometrics data not be used to track people's movements. With less than 50 percent of the sample having heard of, or read about, biometrics, and one in four having experienced biometrics, the public is nevertheless enthusiastic that its use will be widespread within a decade.

Publicly available results of Canadian surveys are not as extensive as American ones but the major issues are touched upon, nevertheless. An Ipsos-Reid poll of 1000 Canadians during the first week of October 2001 showed that 80 percent would be willing to provide fingerprints for a national ID, 59 percent would allow the police to randomly stop and search people, 52 percent are ready to give up some of their liberties to fight terrorism, and 61 percent approve of monitoring personal credit purchases. More than 70 percent opposed giving the police and intelligence officials the power to intercept and read e-mail, regular mail, and listen to private phone conversations. While 58 percent felt that terrorism threats outweigh the protection of individual rights and freedoms, 38 percent believed that even with the threat of terrorism the Charter of Rights and Freedoms should be respected and enforced.[71]

In September 2001, EKOS polling in Canada showed similar results, with one additional finding. Whereas 40 percent of all Canadians disapprove of airport check-in times increasing by one to two hours, among visible minorities it is 58 percent, and for non-visible minority Canadians the proportion is 38 percent. Undoubtedly, this is a statistically significant difference, and it underscores suspicion among visible minorities that profiling is primarily directed against them.[72]

Two years later, Pollara discovered that 73 percent of Canadians were in favour of a biometrics ID card, and in excess of 80 percent supported the use of biometrics in passports, airports, government programs, and border crossings, even though the public knew very little about the details of the

technology.[73] However, more than one-third of Canadians thought that the use of ID cards "goes against Canadian values of freedom and fairness," and more than 50 percent said it would reduce privacy. The EKOS poll of the same year was more substantial in its scope, although the overall picture that emerges is the same.[74] Only 15 percent knew what the term biometrics meant. There was greater support for voluntary, as opposed to mandatory government introduction of the ID card. The survey did offer some contradictory interpretations. For example, although a minority of Canadians (around 12 percent) thought that Canada would be exposed to a terrorist attack, and fewer (2.5 percent) thought they personally would be affected, around 45 percent agreed with the statement that "there is a serious problem with groups supporting terrorist activity in Canada," and 61 percent agreed with the statement that "given the potential of terrorism, the Government of Canada should be given special (extraordinary) powers to deal with possible terrorism-related offences."

As evident in the order of the questions, the EKOS survey tapped an implicit association between immigrants and terrorism in the minds of the public, even though national data in Canada show that immigrants have substantially lower crime rates than native-born Canadians. For example, the lead question asked if respondents thought there were "too many immigrants" in Canada, to which one third answered in the affirmative. From there on, the survey proceeded to ask a battery of questions on terrorism. The Standing Committee on Citizenship and Immigration spotted a similar, though more severe, problem in another survey that was carried out in October 2003 by COMPASS/National Post. The survey asked "do you see the terrorist threat from Islamic extremists as more serious than most threats," and "should people in Canada who are accused of being terrorists have the same rights as accused terrorists?" To its credit, the Committee saw the contaminating effect and dismissed the survey because these questions "raised doubt about the usefulness of the response."[75]

Conclusion Fascination with biometric technology is but one recent example in a long history of modernity's eager embrace of technology generally. What makes the technology intriguing is its cyborg nature; the line between

humans and machines is being further eroded. The technology is being used to authenticate one's identity on the basis of digitized biological and behavioural identifiers as if the technology has become an extension of us and we of it, with an algorithm standing in for our biology.

At the governance level, biometric technologies are being promoted with vigour and some notable success as a result of 11 September. They are being marketed as essential tools to be used in conjunction with other surveillance technologies, to reduce risk and enhance security. The combination of public fear, lobbying efforts of the industry, and linkages between political and economic interests, have catapulted the industry to centre stage in the fight against terrorism —an industry that until 11 September was a marginal player in the security field. This development conjures up President Eisenhower's warning of nearly half a century ago concerning the rise of the military-industrial complex and its influence on politics. An addendum to Eisenhower's observation is the emergence in the twenty-first century of a security-industrial complex in which, in the name of security, the state embarks upon population management and control.

If unchecked through proper oversight, far from being a friend of governance and enhancer of privacy, future developments in the application of technology are likely to exacerbate social division. It is clear that the primary targets of biometric technology are people on the move in pursuit of better life chances elsewhere, preferably in the developed world. Policies of exclusion and categorization of national groups do not bode well for multicultural societies, among which Canada occupies a special place.

What emerges from the above analysis is the public's willingness to accept a tradeoff between privacy concerns and promises of security through technology. Little attention is being paid to unsubstantiated claims of the technology and its unintended consequences. All of this is being made possible through three main convergent forces: first, there is little willingness to question the reliability of the technology lest one is accused of being a Luddite and against progress; second, the formidable lobbying campaign, mounted by corporate stakeholders since 11 September, to adopt biometric technology has found more than willing partners in the corridors of power, and third, the use of biometrics for surveillance purposes will contribute to

widening the surveillance net and gathering of personal information that goes beyond security concerns to include aspects of day-to-day governance and administration. Gradually, biometric technology will emerge as a centrepiece in the design and adoption of ID cards, and the administration of so-called high-risk individuals not only at airports and in security places, but in society generally, including the poor, marginal, and vulnerable people.

The 11 September crisis has demonstrated the nature of extreme risk in high modernity, and how risk and insecurity drive political agendas such as the enacting of various antiterrorism legislations after 11 September. Technological dominance and political dominance go hand in hand. The role of the United States as the dominant technological and military power has had significant spillover effects on the way other countries react to terrorism. Because of its proximity to the United States, Canada's increasing use of biometrics, and the enacting of legislation to counter terrorism, will undoubtedly place Canada more firmly within the techno-administrative orbit of the United States. This is becoming clearly evident in the sharing of information and harmonization of administrative and technological measures across entry points between the United States and Canada.

Notes

The research for this study was funded by a strategic grant from the Social Science and Humanities Research Council. The authors are grateful for the helpful comments made on an earlier draft by Fiona Kay, David Lyon, André Mazawi, Norman Macintosh, Vincent Mosco, Abbe Mowshowitz, Reg Whitaker, and an anonymous reviewer.

1. L. Juillett and G. Paquet, *Information Policy and Governance* (Ottawa: University of Ottawa, 2001), http://www.governance.uottawa.ca/background-e.asp#what.
2. C. Parenti, *The Soft Cage: Surveillance in America from Slave Passes to the War on Terror* (New York: Basic Books, 2003).
3. J. Morison, "Democracy, Government and Governmentality: Civic Public Space and Constitutional Renewal in Northern Ireland," *Oxford Journal of Legal Studies* 21/2, (2001), pp. 287-310, p. 289.
4. D. Smith, "From Women's Standpoint to a Sociology for People," in J. Abu-Lughod, (ed.), *Sociology for the Twenty-First Century: Continuities and Cutting Edges* (Chicago: University of Chicago Press, 1999).
5. M. Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Random House, 1979).
6. A. Hunt and G. Wickham, *Foucault and the Law: Towards a Sociology of Law as Governance* (London: Pluto Press, 1994).
7. L. Axworthy, "Canada and Human Security: The Need for Leadership," *International Journal* 11/2, (1997), pp. 183-196.
8. P.K. Manning, *Security in High Modernity: Corrupting Illusions* (Boston: Northeastern University, 2002).

9. *Ibid.*, pp. 2-3.
10. G. Marx, "Measuring Everything that Moves," *Research in the Sociology of Work* 8 (1999), pp. 165-189.
11. Manning, *Security in High Modernity*, p. 11.
12. M. Valverde, "Governing Security, Governing through Security," in R.J. Daniels, P. Macklem, and K. Roach, (eds.), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2002), pp. 83-92, especially p. 85.
13. *Ibid.*, p. 89.
14. US General Accounting Office (GAO), *Technology Assessment Report: Using Biometrics for Border Security* (Washington, DC: 2002).
15. International Biometrics Industry Association (IBIA), *Interest in Biometric Industry Continues to Soar: 120,000 Visit IBIA Website in July 2000* (Washington, DC: 8 August 2000), available at http://www.ibia.org.
16. D. Knights, F. Noble, T. Vurdubakis, and H. Willmott, "Chasing Shadows: Control, Virtuality and the Production of Trust," *Organization Studies* 22/2 (2001), pp. 311-340, p. 325.
17. *Ibid.*, p. 329.
18. *Ibid.*, p. 330.
19. M. McCahill and C. Norris, "Victims of Surveillance," in P. Francis, V. Jupp, and P. Davies, (eds.), *Understanding Victimization*, Forthcoming.
20. M. McTeer, "Privacy Comes First," *The Globe and Mail* (28 June 2001).
21. D. Nelkin and L. Andrews, "Surveillance Creep in the Electronic Age," in D. Lyon, (ed.), *Privacy, Risk and Digital Discrimination* (London: Routledge, 2002), pp. 94-110; E. Zureik, "Theorizing Surveillance: The Case of the Workplace," in D. Lyon, (ed.), *Privacy, Risk and Digital Discrimination* (London: Routledge, 2002), pp. 31-56.
22. D. Birch, "A World Away from the Reality," *The Guardian* (24 January 2002), http://www.guardian.co.uk.
23. J. Lee, "Report Suggests Use of Facial and Fingerprint Scanning on Foreigners," *New York Times* (12 February 2003), http://www.nytimes.com/2003/02/12/technology.
24. Electronic Privacy Information Center (EPIC), *Biometrics Identifiers* (7 January 2003), http://www.epic.org/privacy/biometrics/.
25. B. J. Feder, "Technology and Media: A Surge in Demand to Use Biometrics," *New York Times* (17 December 2001).
26. M. Ciarracca, "Post-9/11 Economic Windfalls for Arms Manufacturers," *Foreign Policy In Focus* 7/10 (2002), http://www.fpil.org.
27. Privacy Commissioner of Canada, *Annual Report 2000-2001* (Ottawa: Government of Canada, 2001).
28. International Biometrics Industry Association (IBIA), *Biometrics and Counter-Terrorism, A Statement by the Board of Directors of the International Biometrics Industry Association* (Washington, DC: 21 September 2001), http://www.ibia@ibia.org.
29. *Ibid.*
30. Visionics, *Protecting Civilization from the Faces of Terror: A Primer on the Role Facial Recognition Technology Can Play in Enhancing Airport Security* (24 September 2001), http://www.visionics.com.
31. J. Sharkey, "The Nation: Class Consciousness Comes to Airport Security," *New York Times* (6 January 2002), http://www.nytimes.com.
32. Visionics, *Protecting Civilization.*
33. *Ibid.*
34. *Ibid.*
35. E. Lichtblau, "Administration Creates Center for Master Terror 'Watch List,"' *New York Times* (17 September 2003), http://www.nytimes.com.
36. Visionics, *Protecting Civilization.*
37. Robert Gailing. "Biometrics in the Workplace," (White Pape, Bioscrypt Inc., Van Nuys, California), p. 2.
38. Nuance, *The Business Case for Speech Recognition. White Paper* (Menlo Park, California: 2000), http://www.nuance.com.

39. Biometric Foundation (BF), "Mission Statement (2002)," available at http://www.biometric-foundation.org/tbfmission.htm.
40. P. Collier, "Executive Director of the Biometric Foundation Testifies on October 12 Before the Senate Subcommittee on Technology, Terrorism, and Government Information," *Biometrics Advocacy Report* III/17 (19 October 2001).
41. *Ibid.*
42. IBIA, *Biometrics Advocacy Report* III/18 (2 November 2001).
43. *Ibid.*
44. CATA Biometrics Group, *Mission and Mandate Statement* (2002), http://www.cata.ca/biometrics.
45. CATA Biometrics Group, *CATA News* (17 January 2002), http://www.cata.ca/biometrics.
46. *Ibid.*
47. Canada, *Government Response to the Report of the Standing Committee on Citizenship and Immigration "Across the Border: Working Together at our Shared Border and Abroad to Ensure Safety, Security and Efficiency"* (2002), http://www.cic.gc.ca/english/pub/hab.html.
48. *Ibid.*
49. *Ibid.*
50. A. Gentleman, "ID Cards May Cut Queues but Learn Lesson of History, Warn Europeans," *The Guardian* (15 November, 2003).
51. Privacy Commissioner of Canada, *News Release. Privacy Commissioner of Canada criticizes CCRA's Plans for "Big Brother" Database* (26 September 2002), http://www.privcom.gc.ca/media/nr-c/02_05_b_020926_2_e.asp?V=Print.
52. Privacy Commissioner of Canada, *Statement of Support from Provincial and Territorial Information and Privacy Commissioners* (12 November 2002) available at http://www.privcom.gc.ca/media/le_021113_e.asp?V=Print.
53. Privacy Commissioner of Canada, *News Release* (9 January 2003), http://www.privcom.gc.ca/media/nr-c/02_05_b_030109_e.asp?V=Print.
54. Privacy Commissioner of Canada, *News Release – Breakthrough for Privacy Rights* (9 April 2003) available at http://www.privcom.gc.ca/media/.
55. D. Schneiderman, "Terrorism and the Risk Society," in R.J. Daniels, P. Macklem, and K. Roach, (eds.), *The Security of Freedom: Essays on Canada's Anti-terrorism Bill* (Toronto: University of Toronto Press, 2002), pp. 64-72.
56. *Ibid.*
57. L. Austin, "Is Privacy a Casualty of the War on Terrorism?," in R.J. Daniels, P. Macklem, and K. Roach, (eds.), *The Security of Freedom: Essays on Canada's Anti-terrorism Bill* (Toronto: University of Toronto Press, 2002), pp. 251-267, especially p. 260.
58. Canadian Centre for Policy Alternatives, *CCPA Analysis of Bill C-36: An Act to Combat Terrorism* (Ottawa: CCPA, 2001).
59. S. Armstrong, "Does Bill C-36 Need a Sunset Clause?" *University of Toronto Faculty of Law Review* 60/1 (2002), pp. 73-78.
60. P. McMahon, "Amending the *Access to Information Act*: Does National Security Require the Proposed Amendments of Bill C-36?" *University of Toronto Faculty of Law Review* 60/1 (2002), pp. 89-101.
61. F. Stalder and D. Lyon, "Electronic Identity Cards and Social Classification," in David Lyon, (ed.), *Surveillance as Social Sorting* (London: Routledge, 2001), pp. 77-93.
62. C. Clark, "Coderre Pushes Ottawa to Adopt National ID Cards," *The Globe and Mail* (9 February 2003).
63. "Why the Proposal for a National Identity Card (editorial)," *The Globe and Mail* (11 February 2003).
64. Citizenship and Immigration Canada Forum, *Biometrics: Implications and Applications for Citizenship and Immigration*, Ottawa (7-8 October 2003); "National ID Card Puts Rights at Risk (editorial)," *Toronto Star* (17 August 2003).
65. Alan Dershowitz, "Should this Man be Assassinated?" *The Globe and Mail* (16 September, 2003).

66. J. Gilliom, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (Chicago: University of Chicago Press, 2001); D. Lyon, *Surveillance After September 11* (Cambridge, England: Polity Press, 2003).
67. M. Davis, "The Flames of New York," *New Left Review* (November/December 2001), pp. 34-50, especially p. 50.
68. Electronic Frontier Foundation (EFF), "Biometrics: Who's Watching You?" (2002), http://www.eff.org/Privacy/Surveillance/biometrics.html.
69. Accenture, *Majority Travelers Continue with Holiday Flight Plans, According to New Accenture Research* (7 November 2001), http://www.accenture.com; Harris Poll, *The Harris Poll #49* (3 October 2001), http:www.harrisinteractive.com/harris_poll/ lates.asp; Los Angeles *Times*, "Los Angeles *Times* Poll Alert (6 September 2001).
70. A.F. Westin, *The American Public and Biometrics*, presented at a conference organized by the National Consortium of Justice and Information Statistics, New York City (5 November 2002), http://www.search.org/policy/bio_conf/Westin%20Final.ppt. See the full findings of the survey at http://www.search.org/policy/bio_conf/Biometricsurveyfindings.pdf.
71. D. Leblanc, "80 percent Would Back National ID Cards," *The Globe and Mail* (6 October 2001).
72. EKOS Research Associates Inc., *Security, Sovereignty and Continentalism: Canadian Perspectives on September 11* (27 September 2001), http://www.ekos.ca/admin/ press_releases/27-sept-2001e.pdf.
73. Public Policy Forum, *Biometrics: Implications and Applications for Citizenship and Immigration*. Background paper prepared for the Citizenship and Immigration Canada Forum, Ottawa (7-8 October 2003).
74. EKOS, *Canadian Attitudes Towards Biometrics and Document Integrity*. Paper presented at the Citizenship and Immigration Canada Forum, Ottawa (7-8 October 2003).
75. Canada, *A National Identity Card in Canada*. Report of the Standing Committee on Citizenship and Immigration (Joe Fontana, Chair: 2003), http://www.parl.gov.ca.