Rising Governmental Use of Biometric Technology: An Analysis of the United States Visitor and Immigrant Status Indicator Technology Program

Lisa Madelon Campbell †

> … the social consequences of new technological systems will always be largely unforeseen and unintended … Human destiny emerges as the unintended consequence of invention. We are performing a grand experiment on ourselves in the complete absence of informed prior consent.[1]

This article explores increased governmental interest in the use of biometric measurements as a means of identifying individuals and tracing their movements. Private industries, of course, are equally interested in biometrics, and often similarly capable of collecting and storing biometric information. For example, merchants in the United Kingdom require customers who pay by cheque to provide a thumbprint as an additional security measure against potential fraud.[2] The issues raised by the use of biometrics in the private sector are somewhat different than those that arise in the public context. This article explores the increased reliance upon individual biometric measurements by governments in general and the United States of America in particular, and analyzes the ensuing implications for the privacy rights of individuals travelling to and living in that country.

Biometric Measurements Defined

Biometrics has been described as "the automatic identification or verification of living human beings based on behavioural or physiological characteristics".[3] It involves taking or recording some of an individual's most inalienable biological parts and using these to identify him or her. The information can be used in two ways:

(1) to verify that the person is who they say they are, by comparing a previously stored biometric measurement to a fresh measurement provided by the individual, or

(2) to identify a person, by comparing their biometric measurement against a larger database of stored measurements.[4]

Biometrics, when used to link an individual to a particular event in time or place, may lend credence to other information that may be available about an individual's identity or activities.[5] The most elemental biometric measurements include hair and eye colour, gender, and skin colour. Photographs will usually record these forms of biometrics. Facial recognition technology involves taking measurements of the contours of a person's face from different viewpoints, and comparing these with images in an electronic database or an image on an identity card. With facial thermography, the heat patterns emanating from each person's face are measured from thousands of angles, creating a "heat" image.[6] Hand geometry measures the hand and the spaces between fingers to generate a dimensional record.[7] More sophisticated biometric information includes measurements of hand geometry, fingerprints, deoxyribonucleic acid (DNA) patterns, and eye iris scans.[8]

The Evolution of Biometrics

Fingerprint technology was developed in the late nineteenth century and is now widely used to verify identification. Today, facial recognition systems used in public areas such as walkways, airports, and sports arenas will alert the monitors of the system when there is a match between an individual's face captured by the camera and a database of photographs.[9]

DNA analysis is currently the most precise biometric measurement possible; because of the finely-tuned nature of the testing, however, it is also the most prone to error.[10] Short tandem repeat (STR) DNA analysis is the method most commonly used in the forensic science context. STR involves counting the number of repeating sequences in a given DNA sample, and performing a statistical analysis of the probability that these repeating sequences will appear elsewhere.[11] While this method of DNA analysis is far more reliable than earlier

†© L.M. Campbell, Counsel, Department of Justice Canada. The views and opinions expressed in this paper, prepared for the 19th Conference of the International Society for the Reform of Criminal Law June 26–30, 2005, Edinburgh, Scotland, are solely those of the author and do not necessarily represent the views and opinions of the Department of Justice.

methods,[12] errors may arise from animal contamination or mixing with other human DNA.[13] The most reliable samples come directly from blood and other bodily fluids; however, DNA may be culled from discarded facial tissues or from postal stamps that have been licked by an individual. Essentially, human beings leave a trail of genetic information wherever they go.

DNA databases help to assess the result of a match between an individual's DNA and DNA found somewhere else.[14] Recent technologies convert biometric measurements into algorithms, which are then used for matching. As is discussed above, the science of biometrics is based upon the statistical likelihood that two measurements are a match. Computer matching techniques have an error rate that necessarily produces false positive results, as well as false negative results.[15] This statistical error rate is significant, because as we will see below, it is one of several potential flaws in collections of biometric information.

Practical and Theoretical Problems in Biometric Applications

Biometric measurements tend to be treated as infallible; however, they are subject to error and they tend to be most reliable when paired with other identifying information. Every reliable method of identification should have these features:

(1) it should measure a fixed and unalterable individual characteristic;

(2) that characteristic should be present in every individual;

(3) that characteristic should be unique to every individual; and

(4) that characteristic should be recordable, such that it can be compared against others.[16]

Many systems of biometric measurement do not yet have common standards, so the tendency is to scan more data rather than less, in order to later accommodate specific data measurements.[17] As well, biometric measurements may not be designed to accommodate the different forms in which individuals will present themselves. Differently-abled persons may confound biometric measurements; for example, someone with a medical condition called pendular nystagmus, which results in a constantly moving iris, cannot be iris-scanned.[18] Unless they are able to take into account every possible variant, biometric measurements will necessarily be flawed.

"Outliers", or departures from the mean, must be factored into every biometric system. For example, a speaker recognition system based upon aural resonance and designed using male subjects will not function in the same way with female subjects, who have a shorter aural resonance time-span. In addition to variations among subjects, environmental factors must also be taken into account. Facial recognition systems may fail if lighting, position, or backgrounds are changed. An individual's fingerprints are never completely identical, and will vary significantly with changes in moisture and temperature.[19] Fingerprints from the same digit may vary considerably due to differences in the pressure applied, or whether there was something on the finger such as moisture or another substance.[20] In an interesting intersect between science and technology, biometric measurement systems may fail when faced with a scientifically engineered body part such as a glass eye or prosthetic hand. Identical twins have the same DNA profiles, and persons in the same family may have DNA that appears very similar.

The problems posed by these potential errors are further compounded when biometric information is compiled into databases, as is generally required in order for it to be useful to governments and other entities. The integrity of databases is essential to producing accurate results, and this integrity may be adversely affected by various factors, including samples from a single individual appearing more than once. For example, it is important that the sampling methods be the same, and that scientists analyzing the data receive the same training and apply the same methods of analysis.

One major assumption underlying DNA databases is that the DNA of the population from whom the samples were taken is sufficiently homogeneous that differences in a given strand of DNA may be interpreted as statistically significant.[21] The scientific exploration of human beings is far from complete. The human genome was sequenced in its entirety in 2003,[22] and scientists have a relatively good understanding of the chemical composition of DNA. Little is known, however, about the human genome's highly complex structure and functions.[23]

There are slight variations in alleles[24] among ethnic groups, although with the increased movement of populations around the globe, it is anticipated that these will decrease over time.[25] Blood relatives may have DNA that is similar in appearance; thus, when one member of a family is required to give a sample to a DNA databank, the potential is there for identifying information about several people to be included in the databank.[26] In fact, at the genetic level, all *homo sapiens* are relatively homogeneous as a species, with more variation apparent within small populations than between major racial groups.[27] As researchers have observed, using genetic information to categorize racial groups is fraught with problems; they advocate for more work on the biological and socio-cultural factors that link genetics to race and ethnicity.[28]

The Privacy Implications of the Use of Biometric Measurements

If privacy is a *continuum*, and inviolability of the physical space in which one lives and travels is at one end, then the other end, and perhaps the most sacrosanct, is the inviolability of the self. This includes not only the physical self, but the self as self-defined. When states use biometric measurements to identify individuals, they are, in a sense, pinning people to their biology. Biology is an almost inescapable aspect of the self.

Most incursions into personal privacy are the result of an exchange of some sort; an individual purchases fuel in order to heat his or her residence, and this in turn creates usage patterns that provide information about him or her. Biological information results from simply existing, and individuals cannot help creating it.

Some view increases in surveillance by biological and other means as dehumanizing, an invasion of personhood, and suggest that "total visibility infantilizes people. It impoverishes their inner life and makes them more vulnerable to oppression from without".[29] From this perspective, people will recoil from certain activities for fear that they will be traced, and if they do engage, they do so in a circumscribed fashion, knowing that they may be continuously monitored.

If, however, privacy is viewed as control over expressive information, an entirely new debate begins.[30] Each use of peoples' personal information can be gauged against whether it encroaches upon that aspect of their self, depending upon whether they have expressed themselves as a parent, a consumer, a voter, or a sexual being.[31] This view is likely the preferable one, given that in modern society, most people with access to it will use technology to express themselves in a multitude of ways, many of which can be recorded or traced.

The difference with biometrics, though, is that one cannot help but exist, and by so doing, continuously emanate expressive data. Perhaps even here, though, technological change will outpace the capacity to trace individuals by virtue of their biology. The co-discoverer of the structure of DNA advocates for germline genetic intervention in humans in order to possibly improve the genome.[32] In the context of an application in the United Kingdom to patent a process to genetically engineer mammals so that pharmaceutical products may be produced in their milk, the applicant seeks the rights to genetically engineered human females.[33]

If individuals want to avoid giving off biological information, they must actively intervene in order to protect it, by covering faces so as not to be identified, covering fingers or wiping surfaces so as not to leave fingerprints, and retrieving tissues with possible DNA in them. It is one thing for biometric measurements to be taken for purposes to which an individual consents. The collection of biometric measurements by governments raises the problem that this information may be used in the future for purposes never contemplated by individuals when they first gave the information. That this could happen is quite possible for two reasons:

(1) *Function creep*: the availability of databases containing biometric information makes them susceptible to other uses and of interest to other entities. Insurance companies, for example, are keenly interested in genetic data that may provide information about whether individuals are likely to develop certain illnesses. Marketing agencies are interested in people's movements and activities for purposes of designing advertising. Banks and other financial institutions are interested in biometric information as a way of adding further security to their transactions. An important aspect of this is that certain biological information may be mined extensively and indefinitely: once a DNA sample is collected, it may be retained and tested several times for different purposes unless checks are put in place.

(2) *Technological advances*: given the rapid pace of technological change, it may be impossible to predict the types of information that may be drawn from a given sample of DNA. While the science of DNA has evolved in the past 20 years, it is far from complete. The Human Genome Project successfully sequenced the entire gene; however, current DNA analysis uses only a fraction of the gene sequence. There are two important and emerging fields of scientific research involving DNA:

   (i) *Genetic diseases* — flaws in the genetic code are now known to contribute to up to 4,000 hereditary diseases, such as cystic fibrosis. Genetic mutations are also associated with predisposition to other illnesses, such as cancer and diabetes.

   (ii) *Behaviour* — genes appear to have some influence on behaviour. Genes have been found to influence sexual behaviour, thrill-seeking, and violent tendencies.[34] While not determinative, genes play a role, along with the environment and other factors, in how individuals conduct themselves.

An example of "function creep" exists in the United States, where 20 states now allow law enforcement agencies to use collected DNA samples in research aimed at improving forensic techniques. This research is partly directed towards the controversial field of examining genes for predictors of criminal behaviour.[35] While there is some suggestion that DNA may play a role in predicting human behaviour, most scientists agree that an approach that focuses solely on genetic *indicia* of behaviour is destined to fail, as it does not consider the essential interaction between genes and the environment:

> Behavior flows from brains that (a) encounter specific environmental stimuli and (b) possess a neural architecture that

> is as importantly shaped by environments as it is by genes. The essential point is that biological processes, properly understood, provide no support for genetically deterministic views of human behavior, whether they arise from political motivations or from misconceptions.[36]

It is unclear whether biometric measurements are considered "data" for purposes of privacy legislation. Danish authorities have decided that there is personal information within human biological material; however, a Norwegian tribunal held[37] that blood samples in a hospital were not personal information within the meaning of that country's *Personal Data Act* of 2000.[38] Most privacy legislation was developed prior to the widespread use of biometrics as a method of identifying citizens, and before technological advancements in areas such as DNA analysis. While many of the natural justice principles underlying most privacy legislation would apply to the collection and storage of biological data, some principles, such as those governing the use of that data, would not. Biometric measurements are subject to uses that may be very different than those that would apply to other types of information, including replicating the biometric, testing it for genetic information, or testing it against information found at a crime scene.

The European *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (the Convention)[39] has, since 1981, been open for signature by any country as long as that country ensures that its national legislation conforms with the principles of the Convention. Of the natural justice principles underlying the Convention, one of the most significant is that data collected must be accurate, sufficient for the purpose for which it was collected, and retained only for as long as required.[40] The Convention allows for the uninterrupted flow of personal information between countries party to the Convention.

While not specifically addressing human biological samples, the 1995 European Commission's *Directive on data protection* in defining "identifiability" provides that it includes identification by reference to factors specific to physical and physiological identity.[41] The Commission's comments leading up to the finalization of the directive show that it intended that the term "personal data" be broadly interpreted to encompass fingerprints and genetic characteristics.[42] The Project Group on Data Protection, a consultative body composed of information experts from the member countries, prepares reports on biometrics.[43]

Governmental Interest in Biometrics To Track Individuals

States have long used individual identifiers to enable them to track the movements and whereabouts of citizens. In the Roman Empire, soldiers, slaves, and citizens were identified by means of tiles; the South African passbook was part of that country's apartheid system.[44] In the wake of the terrorist attacks in the United States in September 2001, international and national government organizations enacted legislation and adopted other measures aimed at combating terrorist acts, and governments the world over have shown an unprecedented interest in collecting biological information about individuals.

Of the 15 European Union member states, 11 have national identification cards; in France, it is voluntary, while in other countries, such as Greece and Spain, it is compulsory for citizens to carry an identity card.[45] Thailand's Central Population Database is populated with information linked to a national identity card system. The cards contain facial images, electronic fingerprints, and other personal information, and are linked to an electronic database to which most government agencies have access.[46] There are many countries in which national identity schemes do not exist formally, but rather in a *de facto* sense. Initially developed as a permit to allow individuals to drive vehicles, the drivers' licence in many countries has now become a form of identification used to facilitate a number of transactions unrelated to driving. The Office of the Privacy Commissioner of Victoria describes drivers' licences as a rich source of personal information that is akin to a national identity card.[47]

The United Nations Security Council passed Resolution 1373[48] which, while failing to define terrorism, requires member states to adopt a broad spectrum of measures to combat terrorism. These measures include the sharing of information and restrictions on the movements of terrorists. The UN Counter-Terrorism Committee monitors state compliance with the Resolution.[49] The European Union in 2002 adopted a Framework Decision on Combating Terrorism[50] that contains a broad definition of terrorist acts and requires member states to legislate in compliance with the decision.

The International Civil Aviation Organization has recommended facial recognition as a standard biometric measurement that ought to be included in identity documents, and suggests that each country should be free to add a second biometric of its choice.[51]

Measures aimed at preventing terrorism in Germany empower the country's Office for the Protection of the Constitution and Federal Intelligence Service to track non-citizens by means of a centralized database in which individuals' biometric measurements and other personal information is stored.[52] Similarly, applying Britain's 2001 anti-terrorism legislation, law enforcement authorities may now search suspects without a warrant and collect biometric measurements such as fingerprints.[53]

Immigration officials in the United States, Canada, and at the Israeli–Palestinian border currently use hand geometry technology to identify travellers.[54] In a pilot project between Canada, the United States, the Nether-

lands, and Germany, travellers will be given a card that contains their unique hand measurements.

Proposed U.S. legislation would require microchips with biometric information to be implanted in state driver's licences, in order to render licences more secure and less susceptible to forgery. Opponents characterize the move as a shift towards a *de facto* national identity card.[55] Social assistance recipients in some states in the United States must provide their fingerprints, and fingerprints are included in driver's licences in California.[56]

Citizens of the United Kingdom are arguably the most watched people on the planet. Being stopped by law enforcement authorities in the United Kingdom may mean having one's fingerprints and DNA collected, whether or not one is charged or even arrested. The United Kingdom's national DNA database contains the genetic profiles of over two million people.[57]

When biometric information is included in national identity cards, governments may more easily trace individuals' movements within national borders. The principal purpose of an identity card system is to link an individual to a body of data. Identity checks themselves generate data by creating information about the location of an identifiable individual at a given time and place. This in turn impacts upon privacy and further reduces the possibility of remaining anonymous.[58]

Several authors argue vehemently against the creation of national identity cards with biometric identifiers, suggesting that individual privacy should not be sacrificed for measures that may or may not actually defeat terrorism.[59] With all due respect to these commentators, their arguments reveal a certain naïveté: identity cards are here. As we have seen from the preceding discussion, and will analyze in more detail below, identity cards are comprised partly from information stored in electronic databases, and partly from paper identification already widely in use, such as driver's licences and passports.

The Collection and Use of Biometrics by the U.S. Government

It is important to consider the collection of biometric information by the U.S. government both from within and outside its national borders, because, as will be discussed below, the government is using this information in an integrated manner.

The International Aspect

While there are over 300 air, land and sea ports of entry to the United States, most travellers enter by land.[60] Following the attacks in 2001, the United States enacted various legislative measures aimed at countering terrorism, including the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*[61] (USA Patriot Act), the *Homeland Security Act*,[62] and *Enhanced Border Security and Visa Entry Reform Act*[63] (EBSVERA). Provisions in the first and latter Acts required that biometric identifiers be used in travel documents and that an automated entry and exit data system be developed that would work in concert with other law enforcement and national security databases.[64]

Interestingly, U.S. officials call this capacity for interoperability, which links an entry-exit database to other government databases and allows access by a vast array of U.S. law enforcement agencies, "Chimera".[65] That word, as used in Greek mythology, means a fire-breathing monster, with a lion's head, a goat's body, and a serpent's tail; as used in biology, it means an organism whose cells are not all derived from the same zygote.[66] As is discussed below, it remains to be seen which of the two descriptions is more apt.

Racial, ethnic, and national factors have played a central role in law enforcement measures in the United States since 2001.[67] That year, the United States announced the launch of the National Security Entry-Exit Registration (NSEERS), a program requiring male non-citizens over the age of 16, from certain countries, to provide fingerprints and photographs upon entering the country.[68] NSEERS targeted nationals of primarily Arabic and Muslim countries, and was intended to apply to most foreign visitors by 2005.[69] In 2003, nearly 82,000 male persons immigrating or visiting from predominantly Muslim countries were registered in NSEERS. Their inclusion in NSEERS was based not upon citizenship but rather ethnicity — it was the country in which they were born that was of interest to U.S. officials.[70] While the information contained in NSEERS appears to have been used in approximately 13,000 deportations, officials indicated that the system identified only 11 individuals as having links to terrorism.[71] Five of these 11 individuals were actually charged with a terrorist-related offence.[72]

NSEERS was intended to act in concert with the Schengen Information System, the European Union's automated system containing personal information about migrants and people who are suspected of having committed or witnessed a crime. With over a million entries, the Schengen system contains various types of personal information, including individuals' professions and their sexual orientation.[73]

Another electronic database in the United States, entitled the Student Exchange Visitor Information System (SEVIS), became fully operative in 2003 and stores information on individual foreign students using Internet-based technology.[74]

Formed in 2003, the U.S. Department of Homeland Security (DHS) is statutorily mandated to prevent and respond to terrorism in the United States and reduce its exposure to terrorism. Since its creation, the DHS has been a central actor in various crime prevention initiatives that are arguably unrelated to terrorism as it is

traditionally understood. Under a program called "Operation Predator", the DHS finds and assists in the prosecution of persons involved in child pornography. If those individuals happen to be non-citizens, the DHS also assists in their deportation.[75] DHS is a huge government department, and includes the Bureau of Immigration and Customs Enforcement, the Science and Technology Directorate, the Bureau of Customs and Border Protection, the Transportation and Security Administration, the U.S. Coast Guard, and the Citizenship and Immigration Service.[76] The Border and Transportation Security Directorate alone employs over 20,000 people.[77]

That same year, the Total Information Awareness Program was developed within the Pentagon to

> … imagine, develop, apply, integrate, demonstrate and transition information technologies, components, and prototype closed-loop information systems that will counter asymmetric threats by achieving total information awareness useful for preemption, national security warning and national security decision-making.[78]

Also in 2003, DHS announced that a new program called United States Visitor and Immigration Status Indication Technology System (US-VISIT) will integrate the earlier NSEERS and SEVIS systems. Under the new system, which is scheduled to be fully operational in December of this year, when non-citizens enter the United States through any of the air, sea, or land ports of entry, they will be required to provide fingerprints and photographs, and possibly submit to an iris scan.[79] Using current procedures, once inspectors have scanned two fingerprints and taken a digital photograph of the individual, they will enter the biometric information into a database and compare it against other biometric information already stored there to determine whether there is any information that would render the individual inadmissible. When leaving the United States, non-citizens are required to have their travel documents scanned, their photograph compared, and their fingerprints taken once again. When non-citizens leave the United States, officials from DHS will authenticate identity again, using biometric information, and input the details of the departure information into the database.[80]

DHS officials have commented that they may collect additional biometric information when it becomes possible to deploy technology that would allow for this.[81] Information in the US-VISIT database is intended to be used for general national security purposes, and also to locate, and possibly deport, individuals in violation of their visas.[82] According to DHS, other countries are participating in the implementation of US-VISIT, as are U.S. local and state law enforcement agencies and the U.S. departments of State, Transportation, Justice, and Commerce, the General Services Administration, and the Central Intelligence Agency.[83]

Critics of US-VISIT question both the feasibility and ultimate usefulness of the program. It has been suggested that the intense focus on border security has resulted in the insufficient allocation of resources towards enforcement of immigration laws within the United States, including verifying whether individuals have overstayed their visas. Concerns have been expressed regarding the knowledge requirements and increased training needed by immigration inspectors to operate and search the various databases.[84]

In a 2004 report to Congressional Committees, the U.S. General Accounting Office examined the expenditure plan for the US-VISIT program and found that DHS had not produced either an adequate privacy impact assessment or cost-benefit analysis.[85] Significantly, the report found that DHS had not implemented the usual controls seen with the deployment of vast, costly technological systems, such as independent verification and validation. The report concluded that if these failings were not addressed, their consequences would become even more serious with increases in the size and complexity of US-VISIT.[86]

Most observers agree, however, that the viability of US-VISIT will depend in large part on the integrity of the various databases with which it will be integrated, as well as its compatibility with those databases. For example, the two fingerprint methods used under the current program, while adequate for purposes of authenticating an individual's identity, may not be enough to identify a match in the 10-fingerprint system used by the Federal Bureau of Investigation.[87] Also, while the USA Patriot Act.[88] required the integration of the databases of the former Immigration and Nationalization Services department, the U.S. General Accounting Office criticized those disparate databases as being antiquated.[89]

In a 2005 report on the implementation of the land entry portion of the US-VISIT program, the Office of the Inspector General, an auditing body, identified several problems. Among these are the fact that in its initial stages, US-VISIT captured less than 3% of those non-citizens who entered by land, and the exit aspect of the program at land ports of entry is not finalized.[90]

As well, under the manner in which US-VISIT currently operates, front-line immigration officers must query several databases in order to perform the required verifications. These databases, which contain information obtained by other federal agencies, commercial airlines, and sea carriers, include TIPOFF (a terrorist lookout database), the Arrival Departure Information System (ADIS), the Advance Passenger Information System (APIS), the Biometric Verification System (BVS), and the National Automated Immigration Lookout System (NAILS), among others. These databases are supported by various technology systems, and are not currently integrated with US-VISIT.[91] As a result, the knowledge and training requirements for immigration officers has increased, and the additional searches required often cause significant delays at borders.

DHS expects it will take five to 10 years to transform US-VISIT into a comprehensive system for elec-

tronically tracking foreign persons before they enter the United States, at the point of entry, during their stay, and when they leave. In June of 2004, DHS granted a contract worth US$10 billion to Accenture LLP, which has agreed to act as the "prime integrator" and provide the design, integration, and implementation of existing and new systems.[92] By January 2005, DHS had processed over 18 million people in US-VISIT, resulting in over 2,000 matches with law enforcement databases. Of these, roughly half related to potential criminal activity and half to immigration issues.[93]

The Domestic Aspect

As we have seen above, like many other countries, the United States uses various biometric measurements, such as fingerprints and facial recognition, increasingly and in a routine manner in order to authenticate individuals' identity. For obvious reasons, the collection by the United States of individuals' DNA has been the subject of much discussion. The debate over the compelled production of DNA for inclusion in a databank crystallized recently in the decision of the Ninth Circuit Court of Appeals in *United States v. Kincade*.[94]

In 1993, Thomas Kincade, a decorated Navy Seaman who was experiencing worsening personal and financial difficulties, robbed a bank using a firearm. He pled guilty and was sentenced to 97 months' imprisonment, followed by three years' supervised release. Following his release from prison in 2000, Kincade's urine samples tested positive for cocaine. At his request, the Court ordered treatment in a residential drug treatment program, which Kincade followed; after this he appeared to be rehabilitated and to be getting on with his life.

One of the conditions of Kincade's supervised release, however, was to follow the instructions of his probation officer. In March 2002, pursuant to the terms of the U.S. *DNA Analysis Backlog Elimination Act* (DNA Act),[95] the probation officer asked Kincade to provide a blood sample. The DNA Act requires individuals who have been convicted of certain offences[96] and who are incarcerated, on parole, or on supervised release to provide federal authorities with a tissue, blood, or other bodily sample on which a DNA analysis can be performed. Like other analysts, the Federal Bureau of Investigation prefers DNA information from blood samples because it is more reliable than that obtained from other sources. Thus, the guidelines specify that a blood sample be provided.[97]

Kincade refused to provide a blood sample, explaining that he preferred not to for personal reasons. He consulted with his lawyer, and did not present for the scheduled drawing of a blood sample. Kincade was arrested and imprisoned for violating the terms of his release. He filed suit against the U.S. Federal Government, alleging that the DNA Act violated the U.S. Constitution's Fourth Amendment, which guarantees against unreasonable search and seizure. The first level of court to hear his case ruled that Kincade's refusal to provide a blood sample was indeed a violation of the terms of his release. A three-judge panel of the Ninth Circuit Court of Appeals reversed this decision 2–1, concluding that compelling production of a blood sample was a search within the meaning of the Fourth Amendment and that the government must establish individualized suspicion before being permitted to conduct such a search.

In 2004, the Ninth Circuit voted to withdraw the panel's decision and have the case re-heard by 11 judges. In a close 6-5 ruling, the 11 judges ruled in favour of the government, finding that:

> In light of conditional releasees' substantially diminished expectations of privacy, the minimal intrusion occasioned by blood sampling, and the overwhelming societal interests so clearly furthered by the collection of DNA information from convicted offenders, we must conclude that compulsory DNA profiling of qualified federal offenders is reasonable under the totality of the circumstances.[98]

The dissenting judges voiced serious concerns, and would have ruled that programmatic, suspicionless searches were constitutionally unreasonable. They observed that DNA information contained in the Combined DNA Index System (CODIS) has the potential to reveal information about individuals' genetic defects, predisposition to diseases, and possibly sexual orientation:[99]

> When democratic values are lost, society often looks back, too late, and says when did this happen — why didn't we understand before it was too late? Today's decision marks one of those turning points — a fatally unwise and unconstitutional surrender to the government of our liberty for the sake of security, and, should the plurality theory ever become law, the establishment of a doctrine that would leave us without the legal tools to halt further abolition of our privacy rights. The compulsory extraction of blood samples and the maintenance of permanent profiles of American citizens is, unfortunately, the beginning not the end.[100]

The *amicus brief* filed by the Electronic Privacy Information Center with leave of the Court, but without consent of the parties, made the observation that the collection of DNA samples in a relatively accessible national database raises the prospect that the samples may be used in the future for purposes other than those for which they were collected.[101]

Each of the 50 states in the United States has a DNA databank and over half authorize law enforcement agencies to retain DNA samples after profiling has been completed.[102] Three states allow the collection of DNA from persons who have merely been arrested for an offence.[103] U.S. law enforcement officials have also resorted to the use of what some call "genetic dragnets";[104] they approach the family, neighbours and friends of the victim of a violent crime and ask for buccal swabs.[105]

In 1994, the federal government established CODIS, through which law enforcement officials across the United States may access DNA information collected from local, state, and federal law enforcement agen-

cies.[106] The number of profiles in CODIS has grown exponentially; in 2000, there were slightly more than 200,000 profiles, and four years later, there were over a million and a half profiles.[107] CODIS lacks uniformity: each state has differing technical standards and different criteria as to which offences result in a DNA sample being compelled from a convict.[108]

CODIS information is referenced within the National Criminal Information Center (NCIC), another law enforcement database. NCIC is the largest database of criminal history in the United States, with information about more than 52 million people. NCIC is referenced millions of times a day. Fields in NCIC indicate whether a DNA sample from an individual is available, and provides the CODIS file number. NCIC interfaces with the US-VISIT program.[109]

Conclusion and Recommendations

It is clear from the above discussion that the U.S. government is compiling vast amounts of biometric information, including genetic information, in electronic and searchable form, primarily from certain ethnic minorities. Described by some as a "new penology" that has arisen in the United States since September 11, 2001, current profiling is an attempt by the state to manage risk based upon group ethnic characteristics.[110] Aside from the unsettling prospect of a government openly engaging in racist behaviour, this risk management strategy appears to be based upon faulty assumptions, given that persons who engage in terrorist activities often operate using their own identity, an identity that up until the point of the terrorist act, was not associated with any criminal activity,[111] and, as was discussed above, biometric information is not a predictor of human behaviour.

The arrest rate for African-Americans in the United States is four times that of Caucasian-Americans, and their incarceration rate is seven times higher.[112] One author has observed that the collection of DNA samples in this context will result in DNA being collected predominantly from African-Americans, thus increasing the disparity in conviction rates among the two groups.[113] As well, so-called "junk DNA" was deliberately chosen for inclusion in the CODIS databank because it was originally thought not to contain information about an individual's physical or medical characteristics. It is now known, however, that DNA samples derived by the short tandem repeat technology that the Federal Bureau of Investigation uses may provide information about an individual's race or gender, among other things.[114]

While the National Institute of Standards and Technology, in its report to the U.S. Congress, concluded that the collection of biometric information from non-citizens in the form of fingerprints and facial photographs — as opposed to DNA — raised no serious privacy concerns,[115] it is unclear whether consideration has been given to the impact upon privacy and legal rights that the integration of the various databases may have.

Biometric measurements are increasingly prevalent as a means of identifying and tracing individuals. In a world in which technological developments make the analysis of vast amounts of information at a rapid pace possible, and in which governments concerned with security issues seek to positively identify individuals, biometrics play an important role. Biometric measurements have potential flaws, however, that must be taken into account when designing the massive technological systems into which they will be fed. When relying upon the results that those systems produce, it is essential to take into account statistical error rates. This is particularly the case when the results relied upon emanate from a combined database, where the original information was collected from varying systems, and using different criteria.

The significant potential privacy implications must also be addressed. Existing privacy legislation and information-sharing agreements were in the main designed prior to the advent of the widespread use of biometrics. National legislation and information-sharing arrangements, as well as international agreements, must be revisited with a view to establishing protocols for the collection, use, and dissemination of biometric information in a manner that protects, to the extent possible, the privacy and integrity of the individual from whom it was originally taken.

Notes:

[1] Alan Lightman, Daniel Sarewitz and Christina Desser, eds., "Introduction" *Living with the Genie, Essays on Technology and the Quest for Human Mastery* (Washington, D.C.: Island Press, 2003) at 2, 4.

[2] "Ever feel you're being watched?" *The Independent* (13 August 2003, edition 3) Science & Technology ["Ever feel you're being watched"].

[3] *Ibid.*, definition used by Prof. James L. Wayman, San José State University.

[4] U.S., Electronic Privacy Information Center, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*, (Washington, D.C.: Electronic Privacy Information Center, 2003) at 44.

[5] Dr. Wilson Wall, *Genetics and DNA Technology: Legal Aspects*, (London: Cavendish Publishing Ltd, 2002) at 109.

[6] David Banisar, "Big Brother Goes High Tech" (Spring 1996) 56 *CovertAction Quarterly*, online: Media Awareness Network <http://www.media-awareness.ca/english/resources/articles/privacy/big_brother.cfm>.

[7] *Ibid.*

[8] Daniel J. Steinbock, "National Identity Cards: Fourth and Fifth Amendment Issues", (2004) 56 *Fla. L. Rev.* 697.

[9] Steven Brandl, "Back to the Future: The Implications of September 11, 2001 on Law Enforcement Practice and Policy" (2003) 1 *Ohio St. J. Crim. L.* 133.

[10] Wall, *supra* note 5 at 53.

[11] *Ibid*., at 69.

[12] *Ibid*., at 76.

[13] *Ibid*., at 70.

[14] *Ibid*., at 97.

[15] Privacy and Human Rights 2003, *supra* note 4 at 44.

[16] Wall, *supra* note 5 at 1, 2.

[17] "Ever feel you're being watched?", *supra* note 2.

[18] *Ibid.*

[19] *Ibid.*

[20] Wall, *supra* note 5 at 11.

[21] Wall, *supra* note 5 at 103.

[22] See online: National Human Genome Research Institute www.nhgri.nih.gov.

[23] Francis S. Collins, Eric D. Green, Alan E. Guttmacher and Mark S. Guyer, "A Vision for the Future of Genomics Research", (24 April 2003) 422 (6934) *Nature* 835.

[24] The variant form of a gene or DNA sequence that can exist at a particular location on a chromosome.

[25] Wall, *supra* note 5 at 111.

[26] Jill C. Schaefer, "Comment: Profiling at the cellular level: the future of the New York State DNA Databanks" (2004) 14 *Alb. L. J. Sci. & Tech.* 559 at 563.

[27] Owen D. Jones and Timothy H. Goldsmith, "Law and Behavioral Biology", 105 *Colum. L. Rev.* 405, at 495 [Jones and Goldsmith, "Law and Behavioral Biology"].

[28] Collins *et al*., *supra* note 23.

[29] Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future" (1995) 11 *Santa Clara Computer & High Tech. L. J.* 27 at 40.

[30] Stan Karas, "Privacy, Identity, Databases" (2002) 52 *Am. U. L. Rev.* 393.

[31] *Ibid.*

[32] Lightman *et al*., *supra* note 1 at 107.

[33] *Ibid.* at 123.

[34] Leroy Hood and Lee Rowen, "Genes, Genomes and Society" in Mark A. Rothstein, ed., *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, (New Haven: Yale University Press, 1997).

[35] Schaefer, *supra* note 26 at 576.

[36] Jones and Goldsmith, "Law and Behavioral Biology", *supra* note 27 at 425.

[37] Norwegian Data Protection Tribunal, Case 8/2002, online: <http://www.personvernemenda.no/klagesaker/nrVII2002.html>.

[38] Norway, *Personal Data Act* (2000) No. 31, online: <http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.doc>.

[39] *Convention for the Protection of individuals with regard to the automatic processing of personal data*, 28 January 1981, E.T.S. 108 (entered into force: October 1985).

[40] Council of Europe, "Legal Affairs: Data Protection," *Ibid*., see online: Council of Europe <http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection>.

[41] EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L. 281/31, Art. 2(a).

[42] Dr. Lee A. Bygrave, "The body as data? Reflections on the relationship of data privacy law with the human body" (speech given at the Office of the Victoria Privacy Commissioner Conference, Melbourne, 8 September 2003), online: Privacy Victoria <http://www.privacy.vic.gov.au>.

[43] Council of Europe, *supra* note 40.

[44] Banisar, *supra* note 6.

[45] Philip Martin and Susan Martin, "International migration and terrorism: prevention, prosecution and protection", (2004) 18 *Geo. Immig. L. J.* 329.

[46] Simon Davies, "Sidebar: The Repression Trade" in Banisar, *supra* note 6.

[47] Andrew Hayne, "Counter Terrorism in Australia: the identity imperative" (2003) 3 *JIJIS* 108.

[48] U.N. SCOR, 56th Sess. 4385th Mtg., U.N. Doc. S/Res/1373 (2001), online: <http://www.Tin.org/Docs/scres/2001.htm>.

[49] Kim L. Scheppele, "Other People's Patriot Acts: Europe's Response to September 11" (2004) 50(1) *Loy. L. Rev.* 89.

[50] Council of Europe, *Framework Decision on Combating Terrorism*, Doc. 2002/475/JHA [13 June 2002] O.J. (L 164) at 3.

[51] "Ever feel you're being watched?", *supra* note 2.

[52] Scheppele, *supra*, note 49.

[53] *Ibid.*

[54] Angela Jarvis, "Are Privacy Rights of Citizens Being Eroded Wholesale in Biometric Identification" (18 March 2002) *Alan D. Gold Collection of Criminal Law Articles*, ADGN/2002-353 (QL).

[55] Sylvia R. Lazos Varga, "Missouri, the 'War on terrorism', and Immigrants: Legal Challenges Post 9\11", (2002) 67 *Missouri L. Rev.* 775 at 8.

[56] Banisar, *supra* note 6.

[57] Ralph Maddocks, "UK ID Card: They're at it again!", (15 May 2004) *Le Québecois Libre*, No. 142, online: *Le Quebecois Libre* <http://www.quebecoislibre.org/04/040515-6.htm>.

[58] Daniel J. Steinbock, "National Identity Cards: Fourth and Fifth Amendment Issues", (2004) 56 *Fla. L. Rev.* 697.

[59] See, e.g., Bijon Roy, "A case against biometric national identification systems: 'trading-off' privacy without getting security", (2005) 19 *Windsor Review of Legal and Social Issues* at 45.

[60] U.S., Congressional Research Service, Lisa Seghetti and Stephen R. Vina, CRS REPORT FOR CONGRESS: *U.S. Visitor and Immigrant Status Indicator Technology Program* (US-VISIT) (Washington D.C.: Library of Congress, 18 February 2004) at 2 [*CRS Report for Congress*].

[61] Act of 2001, Pub. L. No. 107-56, 111 Stat. 272 (2001) (codified as amended in provisions of 8 U.S.C.) [USA Patriot Act].

[62] Act of 2002, Pub. L. No. 107-296, §§442,451, 6 U.S.C. §§252, 271 (2002).

[63] Act of 2002, Pub. L. No. 107-173, 116 Stat. 553, §§201–203, 8 U.S.C. §§1721–1723 (2002).

[64] CRS Report for Congress, *supra* note 60 at 4.

[65] *Ibid.* at 7.

[66] Lesley Brown, ed., *The New Shorter English Oxford Dictionary on Historical Principles*, Vol. I (Oxford: Clarendon Press, 1993) *s.v.* chimera.

[67] Steinbock, *supra* note 58.

[68] Stephen H. Legomsky, "Immigration law and human rights: legal line drawing post-September 11th: Symposium Article: The ethnic and religious profiling of noncitizens: national security and international human rights" (Winter 2005) 25 *B.C. Third World L. J.*, 161 at 167.

[69] Martin, *supra* note 45.

[70] Susan M. Akram and Maritza Karmely, "Immigration and Civil Rights After September 11: The impact on California: Immigration and Constitutional Consequences of post-9/11 policies involving Arabs and Muslims in the United States: Is Alienage a Distinction without a Difference?", 38 *U.C. Davis L. Rev.* 609 at 628, 660.

[71] Rachel L. Swarns, "More than 13,000 May Face Deportation" *The New York Times* (7 June 2003).

[72] Akram and Karmely, *supra*, note 70 at 628.

[73] Akram and Karmely, *supra* note 70.

[74] Legomsky, *supra* note 68.

[75] Teresa Miller, "Immigration law and human rights: legal line drawing post-September 11: Symposium Article: Blurring the boundaries between immigration and crime control after September 11th" (Winter 2005) 25 *B.C. Third World L.J.* 81 at 99.

[76] *CRS Report for Congress*, *supra* note 60 at 9.

[77] Miller, *supra* note 75 at 119.

[78] U.S., Report to Congress regarding the Terrorism Information Awareness Program: In response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M §111(b) (20 May 2003), online: TIA Report <http://www.eff.org/Privacy/TIA/TIA-report.pdf>.

[79] Legomsky, *supra* note 68 at 170.

[80] *CRS Report for Congress*, *supra* note 60 at 11.

[81] *Ibid.* at.10.

[82] Legomsky, *supra* note 68 at 170.

[83] *CRS Report for Congress*, *supra* note 60 at 9.

[84] *Ibid.* at 20, 21.

[85] U.S., United States General Accounting Office, Report to Congressinal Committees, *Homeland Security: First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed* (GAO-04-586) (Washington, D.C.: General Accounting Office, May 2004) at 3, 4, online: GAO <http://www.gao.gov/cgi-bin/getrpt?GAO-04-586>.

[86] *Ibid.* at 7.

[87] *CRS Report for Congress*, *supra* note 60 at 22.

[88] USA Patriot Act, *supra* note 61.

[89] *CRS Report for Congress*, *supra* note 60 at 21.

[90] U.S., Department of Homeland Security, Office of Inspections, Evaluations and Special Reviews, Richard L. Skinner, Acting Inspector General, "Implementation of the United States Visitor and Immigrant Status Indicator technology Program at Land Border Ports of Entry", (OIG-05-11) (Washington, D.C.: Department of Homeland Security, February 2005).

[91] *Ibid.* at 21.

[92] *Ibid.* at 22.

[93] *Ibid.* at 7.

[94] *United States of America v. Thomas Cameron Kincade*, 379 F. 3d 813 (18 August 2004) [*Kincade*].

[95] Pub. L. No. 106-546, 114 Stat. 2726 (2000).

[96] The list of offences is quite broad, and includes crimes compiled from more than 200 various sections of the *United States Code*. For example, a DNA sample may be required from someone convicted of damaging property of the United States: *Kincade*, *supra* note 94 at 31.

[97] *Ibid.* at 2.

[98] *Ibid.* at 24, O'Scannlain J.

[99] *Ibid.* at 34.

[100] *Ibid.* at 52, Reinhart J.

[101] Motion of Amicus Curiae Electronic Privacy Information Center for leave to file accompanying Amicus Brief, in *United States of America v. Thomas Cameron Kincade*, No. 02-50380, February 27, 2004, p. 2.

[102] Schaefer, *supra* note 26 at 576.

[103] *Kincade*, *supra* note 94 at 5.

[104] Schaefer, *supra* note 26 at 566; see also *Kincade*, *supra* note 94 at 33.

[105] Schaefer, *supra* note 26 at 569.

[106] *Ibid.* at 559.

[107] Electronic Privacy Information Center, *Brief of Amicus Curiae Electronic Privacy Information Center in Support of Appellant, Thomas Cameron Kincade, Urging Reversal* (No. 02-50380) (Washington, D.C.: Electronic Privacy Information Center, 2004) at 5 [EPIC Brief].

[108] Schaefer, *supra* note 26 at 579.

[109] EPIC Brief, *supra* note 107 at 13, 14.

[110] Miller, *supra* note 75 at 99.

[111] Bijon, *supra* note 59 at 45.

[112] Similarly, among the 6.9 million individuals under some form of correctional supervision in recent years in the US, ethnic minorities are disproportionately represented; see *Kincade*, *supra* note 94 at 32.

[113] Schaefer, *supra* note 26 at 576.

[114] *Kincade*, *supra* note 94 at 4.

[115] *CRS Report for Congress*, *supra* note 60 at 21.