comparative research in law & political economy

CLPE

Law Research Institute Research Paper Series

CLPE Research Paper 5/2005
Vol. 01 No. 01 (2005)

Darcie Sherman

Biometric Technology: The Impact on Privacy

Keywords: biometrics, privacy, globalization

Author Contact: Darcie Sherman
London School of Economics,
London, England, 2004
Email: drsherman@rogers.com
Tel. (416) 987-6212

CLPE Research Paper 1/2005
Vol. 01 No. 01 (2005)

Darcie Sherman

BIOMETRIC TECHNOLOGY: THE IMPACT ON PRIVACY

Abstract: The introduction of biometric technology has resulted in a significant shift, which defies tradition and some of the very values that we cherish as a society. Additionally, there have been numerous recent developments, which have facilitated a fundamental global re-assessment of the safety and security needs of our communities. Other challenges, like the delivery of government-granted social services, have resulted in governments looking for ways to ensure entitlement prior to the provision of finite resources to individuals.

As technology is increasing in sophistication, it is being deployed in novel and creative ways to meet some of these new demands. However, where technology collides with individual rights and freedoms, we are required to examine the utilization of technologies to determine whether the use is proportionate to the alleged benefits. We are similarly compelled to decide whether there are less intrusive means to achieving the stated ends. This inquiry is even more relevant in the face of the new, seemingly global employment of biometric technology and the rationale behind governments developing dependence on this new machinery.

This paper will examine (i) what biometric technology is; (ii) why it has become so popular; (iii) how biometric technology is being applied in every day use; and, (iv) the advantages and disadvantages of biometric technology. This assessment will occur in the context of the impact that this new technology is having on privacy and the privacy rights of individuals.

I. INTRODUCTION

Changes, and the challenges that they often bring with them, sometimes result in a significant shift in the way that things have historically been done. When new technology is factored into this equation, the outcome can be a massive transformation, which defies not just tradition but also some of the very values that we cherish as a society.

There have been numerous developments recently, which, have resulted in a fundamental global re-assessment of the safety and security needs of our communities. Other challenges, like the delivery of government-granted social services, have resulted in governments looking for ways to ensure entitlement prior to the provision finite resources to individuals.

As technology is increasing in sophistication, it is being deployed in novel and creative ways to meet some of these new demands. However, where technology collides with individual rights and freedoms, we are required to examine the use of technologies to determine whether the use is proportionate to the alleged benefits. We are similarly compelled to decide whether there is a less intrusive means of achieving the stated ends. This inquiry is even more relevant in the face of the new, seemingly global employment of biometric technology and the rationale behind governments developing dependence on this new machinery. It is incontrovertible that this is the new future – what is not clear is whether biometric technology is a panacea or a placebo for the current maladies of society.

This paper will examine (I) what biometric technology is; (II) why it has become so popular; (III) how biometric technology is being applied in every day use; and, (IV) the advantages and disadvantages of biometric technology. This assessment will occur in the context of the impact that this new technology is having on privacy and the privacy rights of individuals.

I.1 WHAT ARE BIOMETRICS

Biometrics have been described as "the science of identifying people based on their physiological and behavioural characteristics."[1] Other commentators have defined biometric technology as "generating a readable body: it transforms the body's surfaces and characteristics into digital codes and ciphers to be 'read' by a machine."[2] Still others contend that "biometrics are automated methods used to recognize people based on behavioural characteristics. Biometrics uses immutable personal characteristics, such as facial features, fingerprints, and retinal patterns, to establish and authenticate identity.[3]

For the purposes of this paper, biometrics will be defined as referring to "the measurement and analysis of unique physical or behavioural characteristics (as fingerprints or voice patterns) especially as a means of verifying personal identity."[4] The emphasis here is on the utilization of an individual's unique, immutable physical characteristics as a means of verifying an identity or identifying someone who is unknown.

According to Kamini Bharvada, "verification involves confirming or denying a person's claimed identity and identification is where one has to establish a person's identity."[5] Identification *verification* process works by comparing two biometric representations, "usually called 'templates,' and decide whether

---

[1] Robin Feldman, '*Considerations on the Emerging Implementation of Biometric Technology*,' 2003, 25 Hastings Comm. & Ent. L.J., p.1.
[2] Irma van der Ploeg, '*The Illegal Body: 'Eurodac' and the Politics of Biometric Identification*,' 1999, Ethics and Information Technology, 1: p.1.
[3] Mark G. Milone, '*Biometric Surveillance: Searching for Identity*,' 2001, 57 Bus. Law, p.1.
[4] Merriam Webster, Collegiate Dictionary, 11th Ed., (Merriam Webster Inc., Massachusetts, 2003).
[5] Kamini Bharvada, '*Electronic Signatures, Biometrics and PKI in the UK*,' 2002, International Review of Law, Computers and Technology, 16(3), p.270.

they are the same or not."[6] This is referred to as a one-to-one match and is used to allow specific individuals who have pre-authorized access, admission. According to Tomko's example of a bank machine, a one-to-one search may be

> Used when we are accessing such things as our bank machine….we want some form of control to serve as a gateway to let you and only you in, and keep all others out. In these activities though, we are not searching a database to identify you. We are actually authenticating your eligibility to access the bank machine.[7]

By contrast, a "one-to-many" search "requires the system to read a person's biometrics and scan a large database to find a match."[8] This search "compares a specimen to large number of stored templates and checks whether the database contains a matching one."[9] This investigation is typically used when the individual's identity is unknown and their biometric template is compared against a database of other similar templates. Tomko asserts that "in all cases, your fingerprint pattern, or a derivative of that pattern is stored in a database file and the one-to-many search strategy is an identification process."[10]

The Electronic Frontier Foundation ("EFF") states that "all biometric technology systems have certain aspects in common. All are dependent upon an accurate reference or "registration" sample. If a biometric system is to identify a person, it must first have this sample positively linked to the subject, to compare

---

[6] Irma van der Ploeg, '*Biometrics and Privacy: A Note on the Politics of Theorizing Technology*,' Information, Communication & Society,' 2003, 6:1, p.86.
[7] Dr. George Tomko, '*Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy*?' Presented at the Privacy Laws & Business 9th Privacy Commissioners'/Data Protection Authorities Workshop, 1998, Online: <http://www.dss.state.ct.us/digital/tomko.htm>, p.2.
[8] *Supra*, note 1, p.2.
[9] *Supra*, note 6, p.86.
[10] *Supra*, note 7, p.2.

against."[11] The EFF further suggests that "modern biometric identification systems, based on digital technology, analyze personal physical attributes at the time of registration and distil them into a series of numbers. Once this reference sample is in the system, future attempts to identify a person are based on a comparison of a "live" sample and the reference sample or samples."[12] The registration requirement is essential regardless of type of biometric being utilized. There are many different systems currently being used with additional structures under development. As a result, a review of some of the current biometric technology may help to clarify the importance of the enrolment process.

I.2 FINGERPRINTING

According to the EFF, fingerprinting is a highly familiar and well-established biometric science. The traditional use of fingerprinting, of course, has been as a forensic criminological technique, used to identify perpetrators…this comparison uses the unique features of any given fingerprint, including its overall shape, and pattern of ridges, valleys, and their bifurcations and terminations to establish the identity of the perpetrator."[13] The EFF claims that with "modern biometrics, these features called fingerprint minutiae, can be captured, analyzed, and compared electronically, with correlations drawn between a live sample and a referenced sample, as with other biometric technologies."[14]

Bharvada asserts that "fingerprints are the most widely used biometric and have the advantage of being cheaper and simpler than most other biometrics. They are of course useful to combat

---

[11] Electronic Frontier Foundation, '*Biometrics: Who's Watching You?*,' Online: Electronic Frontier Foundation, <http://www.eff.org/privacy/surveillance/biometrics>, p.7.
[12] *Ibid*., p.7.
[13] *Supra*, note 11, p.10.
[14] *Ibid*., p.10.

identity fraud…"[15] However, while fingerprints are regarded as reliable, changing only in size with age, being highly resistant to modification or injury and difficult to forge,[16] there is a certain stigma that is attached to the use of fingerprints due to their lengthy association with criminals and crime. As a result, people may be less inclined to willingly participate in systems, which use this technology and any discussions around fingerprinting social assistance recipients or asylum seekers invariably meets with resistance.

I.3 HAND GEOMETRY

According to Feldman, "hand geometry technology creates mathematical pattern abstractions using data derived from the length, width, thickness, curvature and surface area of the hand and four fingers. The quality of the enrolment image will affect how often the system falsely rejects the individual in the future…"[17]

The EFF contends that hand geometry is "the most ubiquitous electronic biometric system."[18]

> The hand geometry-based systems require the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured…the human hand presents a sufficiently peculiar conformation of anatomical features to enable authentication, but is not considered sufficiently unique to provide full identification….a simple hand geometry system will measure length and thickness of digits, width of the palm at various points and the radius of the palm. This results

---

[15] *Supra*, note 5, p.269.
[16] *Supra*, note 11, p.10.
[17] *Supra*, note 1, p.4.
[18] *Supra*, note 11, p.9.

> in a relatively simple identification that can be expressed in a very simple, compact string of data. [19]

The EFF asserts that with respect to the deployment of "traditional hand geometry systems, they have typically found acceptance in applications requiring verification of an identity, rather than a full proof or establishment of an identity."[20] These are characteristically situations where an individual is endeavouring "to prove or disprove their membership in a relatively small group of people..."[21] However, "when the stakes are high, these systems are not relied on exclusively to confirm identity; rather they are used to provide an additional layer of security above and beyond… existing security systems." [22]

I.4 IRIS AND RETINA SCANNING

The human eye is believed to present "two features with excellent properties for identification. Both the iris (the coloured part visible at the front of the eye) and the veins of the retina (the thin film of nerve endings inside the eyeball that capture light and send it back to your brain) provide patterns that can uniquely identify an individual."[23]

Of the two, "retinal scanning is the older technology, and requires the subject to look into a reticle and focus on a visible target while the scan is completed."[24] The purpose of this scan is to allow the system to "analyze the patterns of veins occurring in the back of the eye."[25] Naturally, its regarded as "one of the more intrusive

---

[19] *Ibid*., p.9.
[20] *Supra*, note 11, p.10.
[21] *Ibid*, p.10.
[22] *Supra*, note 11, p.10.
[23] *Ibid*, p.11.
[24] *Supra*, note 11, p.10.
[25] *Supra*, note 1, p.4.

biometric technologies, with some subjects reporting discomfort at the scanning method." [26]

By way of contrast, the iris scan "uses an infrared light to identify and create mathematical abstractions of patterns in the coloured tissue around the centre of the eye."[27] The "pattern of lines and colours on the eye are…analyzed, digitized and compared against a reference sample for verification."[28] According to the EFF, the iris recognition has an advantage in ease of use, in that it merely requires the subject to look at a camera from a distance of three to ten inches.[29]

Finally, iris scanners are considered by some to be "by far the most reliable biometric, but relatively expensive."[30] However, to their merit, "iris scans are painless and can be carried out without the subject even noticing."[31] Of course, this illustrates one of the privacy concerns of opponents of this technology.

I.5 FACIAL RECOGNITION

The EFF maintains that facial recognition sprung into the national spotlight during the 2001 Super Bowl, when Tampa police scanned the faces of game fans without their knowledge for the purpose of spotting terrorists in the crowd. Facial recognition remains one of the more controversial biometric technologies because of its very unobtrusiveness. With good cameras and good lighting, a facial recognition system can sample faces from tremendous distances without the subject's knowledge or consent.[32]

---

[26] *Supra*, note 11, p.11.
[27] *Supra*, note 1, p.5.
[28] *Supra*, note 11, p.11.
[29] *Ibid*., p.11.
[30] *Supra*, note 5, p.270.
[31] *Ibid*., p.270.
[32] *Supra*, note 11, p.11.

According to Susan McCoy, "the fundamental principle behind facial recognition technology is that each person's face can be numerically coded and then compared to a database of thousands of other identities of either known criminals or authorized personnel, in nearly real-time."[33] The EFF states that

> Most facial recognition technology works by one of two methods: facial geometry or eigenface comparison. Facial geometry analysis works by taking a known reference point (for example, the distance from eye to eye), and measuring the various features of the face in their distance and angles from this reference point. Eigenface comparison uses a palette of about 150 facial abstractions, and compares the captured face with these archetypal abstract faces.[34]

According to Bridget Mallon, the technology was formulated in the early 1990's as a U.S. Department of Defence initiative called the FERET program. The program was designed to determine whether it would be possible to use algorithms accurately to measure human faces…. the program concluded in 1998, with private corporations waiting anxiously to capitalize on the new technology.[35] These companies are now in the business of supplying, operating and maintaining this technology for governments and the private sector for use in "public" places.

Bharvada suggests that "facial recognition technology is becoming more widespread because it can exploit existing cameras and databases for facial images from driving licences and passports. Further, unlike other biometrics, facial recognition can operate

---

[33] Susan McCoy, '*O Big Brother Where Art Thou? The Constitutional Use of Facial Recognition Technology*,' 2002, 20 J. Marshall J. Computer & Info. L., p.2.
[34] *Supra*, note 11, p.11.
[35] Bridget Mallon, ' "*Every Breath You Take, Every Move You Make, I'll Be Watching You," The Use of Face Recognition Technology*,' 2003, 48 Vill. L. Rev., p.2.

passively, without people realizing that they are being scanned."[36] There is something about the covertness of this surveillance that occurs without the knowledge or consent of the subjects, that causes the greatest concern and objection of opponents of this technology.

I.6 OTHER ALTERNATIVES

While the discussion thus far has focused on some of the more predominant biometric technology in use, there are some other developments in this field, which are briefly notable. Voice verification is thought to offer an interesting possibility because it works by analysing an individual's fundamental vocal characteristics.[37] The premise is that it would allow remote identification using a phone system, an infrastructure that is already in existence and therefore has zero client side costs.[38] However, voice verification systems are required to account for more variables than other systems such as the compression of a voice captured by cheap microphones like the kind found on phone handsets, background noise and other artefacts. Other problems include the tremendous variability of the human voice due to colds, aging and fatigue.[39] Naturally, there are serious issues around the reliability of this technology.

Finally, according to Bharvada, there are a series of other biometric techniques currently under development, which are noteworthy. Some of these new technologies include analyzing "the sound emitted from the vibration of our major organs and even body odour recognition."[40] It is unlikely that these will be in general public use in the near future but it would certainly be interesting

---

[36] *Supra*, note 5, p.270.
[37] *Ibid*., p.270.
[38] *Supra*, note 11, p.11.
[39] *Ibid*., p.12.
[40] *Supra*, note 5, p.270.

to see the technology that would have to be developed for the registration, capture and analysis of such new techniques.

II. WHY HAVE BIOMETRICS BECOME SO POPULAR

Biometric technology has received significant attention in the last few years and its application in every day use has become considerably more common recently. However, the explanations for this development seem to vary with commentators identifying diverging reasons for this expansion.

II.1 SEPTEMBER 11

According to the EFF, the renewed attention to biometric technology is one of the many reactions to the September 11 tragedy.[41] Mallon asserts that "as a result of the terrorist attacks on September 11, 2001, airports and cities across the country are looking to use new technology to regain a level of safety and security that seems to have been lost. As a result, the biometric industry as a whole, as experienced unprecedented growth over the past few years."[42]

Van der Ploeg adds that "following the events of September Eleventh these security needs have been elevated everywhere to the highest priority level, resulting in a strong push towards high-tech solutions.[43]

II.2 SOCIAL SERVICES ENTITLEMENT

Another reason for the expanding demand for biometric technology comes from the social services sector. Van der Ploeg suggests that "one of the principal domains in which experiments

---

[41] *Supra*, note 11, p.1.
[42] *Supra*, note 35, p.8.
[43] *Supra*, note 6, p.86.

with biometrics are being conducted are departments in charge of social assistance and welfare programs in countries like the USA, Canada, Spain and the Netherlands, which are launching programs for detecting and preventing so-called double-dipping."[44] "Double-dipping" is described as "a kind of fraud that involves the collection of more benefits than one is entitled to, by entering the program under two or more identities. A wide consensus appears to exist concerning the high levels of this type of fraud, and hence concerning the urgency of the need for new identification practices."[45]

According to the EFF, "even prior to September 11…large scale civilian biometric identification systems were being pushed."[46] In the U.S., both "the *Personal Responsibility and Work Opportunity Act* of (1995)…, a welfare reform law, and the *Immigration Control and Financial Responsibility Act* (1996),… an immigration reform law, called for the use of "technology" for identification purposes."[47]

II.3 IDENTITY FRAUD

A related problem to double dipping, which is becoming a widespread predicament beyond the multiple identities used in the social services or immigration context, is the issue of identity theft. Tomko asserts that "identity fraud… is a growth industry. Biometrics are being viewed as a solution to identity fraud because they can be used, not only to positively authenticate, but if one wants, also to track individuals and their transactions."[48] While authentication is certainly a reasonable goal, the ability to be able to track individuals and their transactions adds a level of scrutiny and surveillance that is deeply disconcerting.

---

[44] *Ibid*., p.86.
[45] *Supra*, note 6, p.86.
[46] *Supra*, note 11, p.3.
[47] *Ibid*., p.3.
[48] *Supra*, note 7, p.3.

Another development which existed before September Eleventh, but which has significantly increased since, is a heightened government demand to identify individuals attempting to enter a national border. Nowhere is this more evident than in countries like the U.K. and in particular, the U.S. According to Neda Matar, "using secure identification may also mean preventing national crises. Our need to identify those who enter the United States, manage those who overstay their welcome, and be alerted to terrorist-like patterns of activity has taken on a new level of urgency."[49]

II.4 TRAVEL EFFICIENCY

Mark Milone suggests that the need for accurate and efficient verification of identity has led to the demand for biometric technology. "Biometrics provide the potential for improved security that is particularly important in the international travel context. It allows for stronger access control and strengthened document integrity. Biometrics are also promising in terms of facilitating travel."[50] Biometrically enhanced procedures are believed to enable more efficient border crossings for pre-cleared frequent travellers.

II.5 IMMIGRATION AND ASYLUM SEEKERS

At the other end of the border-protection spectrum is the increasing demand to better identify visitors who enter a country under the pretence of study, those seeking asylum or individuals who have managed to overstay their visits. The U.K. is extremely concerned with processing legitimate asylum seekers and the Home Office has been working to introduce a smart card Application Registration Card for asylum seekers, which would

---

[49] Neda Matar, '*Are You Ready for a National ID Card? Perhaps We Don't Have to Choose Between Fear of Terrorism and Need for Privacy*,' 2003, 17 Emory Int'l. L. Rev., p.11.
[50] *Supra*, note 3, p.2.

contain fingerprint data. Recent reports indicate that this system is "already going live, and could be said to undercut one of the objectives floated for an ID card, the proof by asylum seekers of entitlement to health service treatment."[51] With health care and other social services resources being extremely limited, the British government is particularly concerned with people claiming asylum simply to access free health care services, at the expense of British citizens.[52]

II.6 ANONYMOUS TRANSACTIONS

Finally, with the advent of new technology such as the Internet, digital communications and the global development of e-commerce transactions, business dealings are becoming more anonymous than ever before. According to van der Ploeg,

> With the rapid proliferation of information technologies, data processing, electronic transactions and service delivery affecting everyday life in multiple ways a strong need for new identification practices has emerged. In numerous contexts, technologically mediated and automated economic and social interaction replaces physical and face-to-face encounters, depriving interacting partners of traditional, trusted ways of establishing to each other who they are.[53]

Due to the growing number of online transactions, merchants are never actually meeting with their customer and have no way of

---

[51] The Register, '*Smart Cards, ID Cards, Nice, Nasty, Inevitable?*,' by John Lettice, 4th August, 2003, Online: <http://www.theregister.co.uk/2003/08/04/smart_cards_id_cards_nice>, p.2. (Last accessed on 9 August 2004).

[52] BBC News, UK Edition, '*Health Tourism Rules Unveiled*,' 30 December 2003, Online: BBC <http://news.bbc.co.uk/1/hi/health/3355751.stm>; BBC News, UK Edition, '*Tories Target 'Health Tourism'*,' 1 June 2003, Online: BBC <http://news.bbc.co.uk/1/hi/uk_politics/2954438.stm>. (Last accessed on 14 August 2004).

[53] *Supra*, note 6, p.86.

verifying the identity of their purchaser. This invariably leads to serious trust and security issues, and the potential for fraud and identity theft.

Additionally, Bharvada asserts that "the movement to open network communication systems, such as the Internet poses significant challenges to implementation of a global electronic trading system. Among the most significant concerns are those pertaining to security of the information involved, that is, confidentiality, trust, integrity and availability. The reduction of the risk of fraud and unauthorized access is vital to enable electronic commerce to truly expand on a global scale."[54]

While security is essential to fostering a flourishing electronic commerce environment, it does not go far enough to resolving the issue of the anonymity of the consumer. Biometrics are being touted as the leading solution to the problem of authenticating the identity of the unknown consumer. However, the issue of how and where these new biometric technologies are being deployed is essential to developing a more complete understanding of the technology before examining the advantages and disadvantages that they may pose in relation to privacy.

III. APPLICATIONS OF BIOMETRICS INTO EVERYDAY USE

Biometrics are now being used or deliberated upon for use in a variety of applications. Where a particular biometric is utilized will be contingent on the expense associated with the technology and the relative significance of the place where the technology is being considered for deployment. An examination of how this technology is being employed is important in order to better comprehend the areas which are regarded by government and the

---

[54] *Supra*, note 5, p.266.

private sector as posing a more serious threat which justifies the expenditure for additional security.

Various biometric technologies are being employed in the protection of open and public spaces. Examples of spaces where biometrics are being utilized would include airports, secured buildings which accommodate the government and the private sector, casinos, sporting events and other large open places. According to a recent newspaper report, fingerprint technology appears to still be the technology of choice in certain shopping areas and airports in England.

> Shops in Bracknell, Houslow and other locations around the UK are beginning to experiment with a thumbprint signature scheme requiring customers who pay by cheque to provide a thumbprint as an extra precaution against fraud. London City Airport secures its staff areas with a photo ID pass with a fingerprint embedded in it, which acts as both an ID card and access control card for its 1,600 employees.[55]

By comparison, Philip Agre confirms that the use of facial recognition systems in the public came to public attention when it emerged that fans attending the Super Bowl had unknowingly been matched against a database of alleged criminals, and when the city of Tampa deployed a face-recognition system in the nightlife district of Ybor City.[56] It is interesting to note that in the case of the Super Bowl, spectators were unaware that their faces were being scanned. By comparison, "as people walk down the streets of Tampa, Florida's historic Ybor City, they are greeted by

---

[55] The Independent (London), '*Ever Feel You're Being Watched?; Whether You're Travelling, Shopping, or on the Way to Work, Your Eyes Have it*,' 13 August, 2003, p.1.

[56] Philip E. Agre, '*Your Face is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places*,' 2003, Online: <http://polaris.gseis.ucla.edu/pagre/bar-code.html>, p.1.

signs stating "Area Under Video Monitoring."[57] Informing people that an area is under surveillance re-empowers individuals, permitting them to make a more fully informed decision about whether they wish to attend an area that is being monitored. This is a significantly different situation from where surveillance is occurring surreptitiously.

According to Mallon, the U.S. is not the only country utilizing facial recognition systems. "England was one of the first nations to capitalize on this new technology. Since the fall of 1998, Newham England, a borough of London, began monitoring its citizens with the same face recognition system as used at the Super Bowl…. British officials were so impressed with the new technology that they announced a plan in 2000 to expand its use. They expect to install almost two million cameras across the country to aid law enforcement officials."[58] In a recent article, the estimated number of cameras currently deployed across Britain is 4.2 million.[59] While its true that not all of these cameras will be utilized for facial recognition systems, the front-end technology is certainly in place for widespread deployment when, not if, the government decides to implement its use more broadly.

As previously mentioned, biometrics are also being deployed in the social services sector as "double-dipping" and welfare fraud are growing issues in many countries. In 1997 in the province of Ontario, Canada, the government passed Bill 142, a *Social Assistance Reform Act*, which included the *Ontario Works Act*, 1997, S.O.1997, Ch.25. While this legislation was controversial, the most contentious provisions enabled the government's welfare agents to require that recipients submit to being fingerprinted

---

[57] *Supra*, note 35, p.3.
[58] *Ibid*., p.4.
[59] PoliceOne.com, '*Big Brother Always Watching in Britain, Where Surveillance Cameras Are King*,' by Jane Wardell, **The Associated Press**, 13 August 2004, Online: PoliceOne.com <http://www.policeone.com/policeone/frontend/parser.cfm>. (Last accessed on 18 August 2004).

before receiving any benefits.[60] What was even more astounding was the support that a similar program introduced by the City of Toronto received from the provincial Information and Privacy Commissioner, Ann Cavoukian. Cavoukian suggested that because the encrypted fingerprint scans would be applied in a very defined, narrow purpose and the potential risks to privacy had been considered carefully in consultation with her office, the threat to privacy would be acceptable.[61]

As discussed, in the intervening years since the introduction of these programs, many other countries have either introduced similar programs or are in the process of considering the use of such technology to stop welfare fraud. The threat to individual privacy through the implementation of these systems is palpable.

In terms of immigration and travel, biometric technology is being introduced using a variety of techniques. According to a recent news article, "the biggest revolution is in travel document. Soon all new passports will contain a microchip holding at least one biometric, probably two. The justification for this emanates from the U.S., which in 2002 enacted legislation requiring all "visa-waiver" countries (which includes the U.K.) to begin issuing biometric passports by October 2004."[62] Apparently, the International Civil Aviation Organization ("ICAO") has recommended facial recognition as the standard because, in their view, it is the logical extension of the existing photograph.

---

[60] Welfare Watch, '*Welfare Reform: At What Human Cost?: Ontario Social Safety NetWork*,' Online:
<www.welfarewatch.toronto.on.ca/wrkfrw/humanco.htm>.
(Last accessed on 18 August 2004).

[61] Ann Cavoukian, '*Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look?*' Information and Privacy Commissioner/Ontario, An Address Given by Ann Cavoukian to the Computers, Freedom and Privacy 98 Conference in Austin, Texas. February 1998, Online:< http://www.ipc.on.ca/scripts/index>.
(Last accessed on 7 August 2004).

[62] *Supra*, note 55, p.1.

However, each country is free to add a second biometric of their choice.[63]

For frequent travellers who have been assessed as 'low-risk' travellers, the use biometrics in travel documents is claimed to enable more efficient processing. Travellers will be able to "jump queue and avoid through controls."[64]

Asylum seekers in Europe are faced with the collection of their fingerprints. In 1997, the European Council introduced the '*Eurodac*' system, which created a centralized database of the digitized fingerprints of every asylum seeker over the age of fourteen years, as taken and submitted by every Member State.[65] The stated purpose of *Eurodac* is "to establish the identity of applicants for asylum and of persons apprehended in connection with the unlawful crossing of the external borders of the community….it is also desirable…to allow each Member State to check whether an alien found illegally present on its territory has applied for asylum in another Member State."[66] It is believed that this process will create greater efficiency in the processing of the applications of asylum seekers within the European Community.

Another application of biometric technologies is the renewed efforts by governments in the development of national identification cards. Currently, several countries are exploring the possibility of rolling out a national identity card to be used by all citizens. These cards are believed to be capable of replacing the need for other currently used documents like driver's licences or social security cards.

---

[63] *Ibid*., p.1.
[64] Supra, note 2, p.296.
[65] *Ibid*., p.296.
[66] *Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention*, Official Journal of the European Communities, L 316, section (3).

According to the Canadian Internet Policy and Public Interest Clinic ("CIPPIC"), a national ID card can be broadly defined as a nationwide, all purpose identification document… It would likely come in the form of a plastic card, with a computer chip containing name, date, place of birth and gender of the bearer. Possible additional information would be physical attributes, such as height, eye colour, or other information like current address, a sample signature, academic degrees or stage names.[67] These cards have the possibility of including biometric data, such as a fingerprint or retinal pattern in the card.

Matar contends that the

> Implementation of the card raises two fundamental issues: security and privacy. The identification card can significantly improve national security by providing reliable verification, as well as a common denominator through which agencies can cross-reference their information. Standardized tamper-proof identification cards used by citizens, residents and visitors containing personal information about the cardholder would facilitate this verification and the ability to create watch-lists.[68]

Matar additionally asserts that the cards could also contain the bearer's biometric data while acknowledging that the inclusion of this information would significantly invade the privacy of Americans, as well as visitors. Matar asserts that "implementing a national identification card in the United States for the purpose of meeting our security goals need not cost us our privacy. A delicate balance must be struck between security and privacy interests."[69]

---

[67] Canadian Internet Policy and Public Interest Clinic ("CIPPIC"), '*National ID Cards*,' Online: <http://www.cippic.ca/en/faqs-resources/national-id-cards>, p.2. (Last accessed on 10 August 2004).
[68] *Supra*, note 49, p.2.
[69] *Ibid*., p.3.

National ID cards are currently in use in Belgium, Germany, Greece, Italy, Poland and Spain. According to CIPPIC, "none of the major common law countries (United States, Canada, U.K., Australia and New Zealand) has a national ID card regime. However, like Canada, the U.K. is currently investigating possible ways of introducing either voluntary or mandatory ID cards."[70] In fact, in the U.K. the implementation of a national ID (aka "entitlement") card has been described as Home Secretary David Blunkett's "pet project."[71]

In a recent article, David Blunkett was quoted as saying that he was planning on "pushing on with plan for an ID card, with a draft bill to hit Parliament within months. The ID card will contain biometrics and may be in the wallets of UK citizens by 2007 at the earliest. …the introduction is necessary to give the government better control over immigration and prevent terrorists from using multiple identities.[72] Blunkett, who has been described as "an enthusiastic advocate of the use of biometrics…,"[73] had his plans for the implementation of a compulsory ID card scuttled in November 2003, when the Cabinet rejected his plan.[74] Blunkett's recent comments indicate his determination to proceed with the introduction of a biometric-based, national ID card in the UK with due speed, despite the well-founded objections of opponents and the fact that the technology remains unproven.

---

[70] *Supra*, note 67, p.3.
[71] *Supra*, note 55, p.1.
[72] Silicom.com, '*Biometric ID Card Bill On its Way 'in a Month*,' by Jo Best, 8 April 2004, Online:
<http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39119896,00.htm>.
(Last accessed on 8 August 2004).
[73] *Supra*, note 55, p.1.
[74] The Register, '*UK ID Card Plan –Intro Voluntary, Morph to Compulsory*,' by John Lettice, 6 November 2003, Online:
<http://www.theregister.co.uk/2003/11/06/uk_id_card_plan_intro>.
(Last accessed 9 August 2004).

There is no question that in the face of the new post-September Eleventh reality governments are looking hard for some tool to restore a sense of safety, security and order for their citizens. Biometric technology is regarded by many as the solution. It promises to authenticate and verify unknown individuals. It is purported to prevent identity fraud, stop welfare cheats, identify asylum seekers, and eliminate anonymity in transactions. However, a review of the advantages and disadvantages of biometric technology may provide a more balanced view by allowing for examination beyond these immediate objectives

IV. THE ADVANTAGES AND DISADVANTAGES OF BIOMETRICS

As with other technologies, there are advantages and disadvantages in the application of biometric technology for purposes like security, social services entitlement, immigration, travel and national identity cards. The rationale for examining both the advantages and disadvantages is to determine who in fact benefits from the implementation of these systems -the government and the private sector, and whether there is any benefit for the average person.

IV.1 ADVANTAGES

According to McCoy, "privacy advocates argue that facial recognition technology is not cost effective because additional security staff are required to run the software adequately. Contrary to this argument, the implementation of facial-recognition technology will not create the need to spend capital on more security personnel. Instead, it will make the duties of existing personnel more efficient."[75] McCoy contends that since the system does the actual checking, looking for matches that are merely verified by the human system operator, that additional staff are

[75] *Supra*, note 33, p.9.

not required and as a result, there are greater efficiencies to be realized by utilizing this type of biometric system.

However, human error in determining whether there is a match is not a secure backstop on this system, instead, it is part of the overall process with the facial recognition system, due to the deficiencies of the technology. Since people often change their appearances through age, weight gain or loss, illness, different glasses or hairstyles which may be misinterpreted by the technology, relying on a human to make such a determination has a number of potentially negative consequences for the subject person. Primarily, if the system indicates that there is a match, the onus would then fall on the subject individual to disprove that the image is theirs. Depending on the circumstance, this could lead to embarrassment, and serious inconvenience such as missed flights or denial of access. It is quite possible that additional security personnel and more capital may indeed be required to deal with false matches or rejects.

Matar suggests that national security in the context of preventing terrorism requires database matching and reliable identification. While the latter only refers to a "trustworthy identification with which to track individuals," the former requires the sharing of information between police and government agencies, such as the FBI, CIA and state police departments.[76]

Matar further alludes that a national security card, which utilizes either a centralized or decentralized database, will result in the greater sharing of information between these competing organizations, leading to greater overall efficiency. This view seems rather naïve. Since these organizations have historically had great trouble sharing information or cooperating with each other under regular law enforcement circumstances, it seems unlikely that the introduction of new technology will suddenly foster a new era of sharing and cooperation.

---

[76] *Supra*, note 49, p.11.

Simon Davies points to the advantage of accurate identification of individuals as a major benefit, which follows from the implementation of a biometric technology system. Accordingly, "the accurate identification of individuals is a key concern for many Government agencies and corporations. It is important to them because it contributes significantly to administrative efficiency and the control of fraud, and can offer benefits to clients as well."[77]

In addition, Davies states that some of the declared "potential benefits of an integrated biometrics-based identification system include improvements in the cost of administration; the integrity of identification; the integrity of information; access to information; the speed of delivery of services and benefits; the accuracy and quality of research; and the level of technical security of communications."[78] However, Davies adds that where these technologies are applied to a specific business or administrative function within a particular organization, the implementation is usually successful. Further, "the majority of these success stories have in common a manageable size, a limited geographic spread, a single purpose and modest and easily defined goals. Where biometric technologies are applied to specific purposes, some confidence may be felt in the system's ability to deliver the intended benefits. On the other hand, many failures and disappointments continue to occur, even among seemingly straightforward projects."[79]

Some of the other suggested advantages achieved through the implementation of biometric technology include: verification of identity in a manner that is convenient, more accurate and secure than exists with current methods, and the elimination of the

---

[77] Simon Davies, '*Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine*,' 1994, Information, Technology & People, p.38.
[78] *Ibid*, p.43.
[79] *Supra*, note 77, p.43.

reliance on passwords.[80] It is likewise believed that the integration of biometric technology into passports and Machine Readable Travel Documents, as required by the new ICAO standard, will lead to greater security as these identifications are considered to be harder to falsify or tamper with.

Finally, some commentators believe that the use of biometric technology will improve the "safety and security of every day activities…which is of utmost importance to the general public considering the recent terrorist attacks directed at the innocent citizens of this country."[81] McCoy declares that "this technology is necessary to prevent further terrorist attacks and it should not be dismissed because of a mere potential for abuse when precautions can be implemented."[82]

McCoy concludes by dismissing opponents concerns about the potential privacy violations through use of biometric systems by averring that facial recognition technology does not violate privacy rights because it is merely making a procedure currently used by law enforcement more efficient. In McCoy's estimation, facial recognition technology is akin to matching faces to pictures.[83] Further, facial recognition technology is also similar to fingerprinting, which has been used to identify perpetrators of crimes for over a century…. fingerprinting is a law enforcement procedure…if fingerprinting does not violate the constitution, then neither should facial recognition technology.[84]

IV.2 DISADVANTAGES

The implementation of biometric technology does have some potentially significant benefits in terms of the creation of tamper-

---

[80] *Supra*, note 1, p.5.
[81] *Supra*, note 33, p.5.
[82] *Ibid*., p.5.
[83] *Supra*, note 33, p.8.
[84] *Ibid*., p.8.

proof documents which are not easily falsified; and the prevention of fraud and identity theft by challenging the further use of multiple identities. However, there are some very serious problems with the technology, which raise grave concerns that need to be addressed. To begin with, the potential for increased surveillance and the threat to privacy are enormous.

In terms of surveillance, David Lyon states that one of the responses that occurred following September Eleventh was the extensive tightening of surveillance. The reactions can be compared to

> A prism that puts several things in perspective. One, it is premature to see decentralized and commercial surveillance simply supplanting nation-state power.... Two, reliance on high tech surveillance methods is undaunted by the low-tech attacks or the failure of high tech security systems already in place. While they may not work to curb terrorism they are likely to impede civil rights for citizens who will be even more profiled and screened. Three, the struggle to make mushrooming surveillance systems more democratically accountable and amenable to ethical scrutiny is being set back by panic regimes following September Eleventh.[85]

Examples of increased surveillance include enlarged surveillance of Internet activity, and public spaces by digital video cameras, and the adoption of national identification cards embedded with biometric information. At the same time, governments have weakened traditional legal protections against unauthorized police

---

[85] David Lyon, '*Surveillance After September 11*,' 2001, Sociological Research Online, 6(3), Online: <http://www.socresonline.org.uk/6/3/lyon.html>, p.1. (Last accessed 5 August 2004).

searches and are increasingly turning to private sector databases to access previously collected personal information.[86]

As a result, Lyon suggests that the type of social structure and processes that are evolving as a consequence are an expanding range of the already existing surveillance processes and practices that circumscribe and shape our social existence, and the tendency to rely on technological enhancements to surveillance systems even when it is unclear that they work or address the problems that they were intended to resolve.[87] Post September Eleventh, "it is safe to suggest that the intensity and the centralization of surveillance in Western countries is increasing dramatically…such systems once in place, are harder to dismantle than to install."[88]

According to Lyon, high-tech companies that had been working to develop new technology and waiting for an opportunity to launch their new products, saw September Eleventh as providing just the platform they needed.[89] The problem is that while panicking governments and populaces embraced this new technology, they disregarded several unresolved issues.

> These technologies may be tried but not tested. That is, it is not clear that they work with the kind of precision that is required and thus, may not achieve the ends intended. Two, they are likely to have unintended consequences that include reinforcing forms of social division and exclusion within the countries where they are established. Third, a larger dimension of the technological aspect of surveillance practices is that seeking superior technologies appears as the primary goal. No matter that the original terrorism involved reliance on relatively aged technologies

---

[86] Arthur J. Cockfield, '*Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance*,' 2003, 29 Queen's L.J., p.72.
[87] *Ibid*., p.2.
[88] *Supra*, note 85, p.2.
[89] *Ibid*., p.3.

> –jet aircraft of a type that had been around for 30 years, sharp knives and so on –it is assumed that high tech solutions are called for. Moreover, the kinds of technologies sought …rely heavily on the use of searchable databases, with the aim of pre-empting acts of terrorism by isolating in advance potential perpetrators. [90]

What is clear is that the technology of today is enabling far-greater surveillance, but is not up to the job of pre-empting terrorism or other potentially nefarious behaviour. "Surveillance can only anticipate up to a point, and in some very limited circumstances. However, searchable databases and international communications interception were fully operational on September 10, to no avail. The likely result will be that internal surveillance of citizens by the state will increase. And if 'terrorists' are apprehended it will be by other means."[91] In the meantime, the public, particularly the American public, appears ready to sacrifice their privacy and permit government intrusions into their affairs in the name of safety, security and routing out the "evil doers."[92]

Biometric technology also poses a very serious threat to privacy. Feldman asserts that "biometrics are merely a form of data. Thus, collection of biometric data raises some of the same issues that arise when government agencies or private firms collect any information about citizens."[93] Further, there are two specific issues that relate to the collection of biometric data. "First, some commentators express concern that biometric data could potentially reveal information about health status…second, biometric technology raises for many people the spectre of

---

[90] *Supra*, note 85, p.4.
[91] *Ibid*., p.8.
[92] CNN.com/US, '*Bush Vows to Rid World of 'Evil Doers*,' by Manuel Perez-Rivas, 16 September 2001, Online: CNN <http://www.cnn.com/2001/US/09/16/gen.bush.terrorism/>. (Last accessed on 19 August 2004).
[93] *Supra*, note 1, p.8.

government tracking."[94] The concern is that the collection of biometric information will result in heightened monitoring of individuals.

According to Cavoukian,

> A fingerprint, and the broader family of biometrics…offer irrefutable evidence of one's identity since they are unique biological characteristics which distinguish one person from another, and which can only be linked to one individual. An identifiable fingerprint can act as a powerful unique identifier that can bring together disparate pieces of personal information about an individual. If used as a unique identifier, a fingerprint enables individuals to be pinpointed and tracked. It also creates the potential for personal information from different sources to be linked together to form a detailed profile about the individual unbeknownst to him or her. This presents a clear invasion of privacy; one that most people would object to.[95]

Privacy is said to revolve "around the freedom of choice; without the ability to exercise some reasonable sense of control over the use of one's information, privacy will become but a quaint notion."[96] Matar adds that "privacy is one of the personal attributes that most people innately cherish. We have an instinctive desire to protect ourselves from being overly exposed. We naturally seek to control who knows us personally, who may get to know us well, and who has personal/private information about us."[97]

The sense is that with biometric technology, personal information is gathered and stored easily and surreptitiously

---

[94] *Ibid*., p.8.
[95] *Supra*, note 61, p.1.
[96] *Ibid*., p.2.
[97] *Supra*, note 49, p.7.

without the subject having control or knowledge. Further, and most disconcertingly, the public has no idea who has access to the information being gathered or how it will be used.

Some commentators suggest that "the benefits of implementing facial-recognition technology are far more important than the benefits of rights to privacy in public places."[98] They claim that society is not willing to protect privacy at the price of risking their safety.[99] It has also been asserted that "society is not willing to grant freedom from facial-recognition technology by allowing individuals to have reasonable expectations of privacy in public places. Facial recognition technology is the first step to the larger solution of ending terrorist attacks and decreasing criminal activity."[100]

While the terrorist attacks undoubtedly shook the American psyche to the core, and deeply affected the rest of the world, there is an intense willingness to embrace any technology that might offer even a scintilla of hope in preventing a repeat of the horrors of September Eleventh. Unfortunately, this appears to include a blind faith in untested biometric technology and an eagerness to submit to public authorities and their agents, all of the hard fought rights and freedoms of privacy, without any proof that such a sacrifice is even justified. There is, after all, no evidence that the technology is completely effective or that it would be successful in stopping terrorists and other criminals.

However, reliance on unproven technology and the covert collection of personal information might not be the biggest problem with biometric technology. According to Cavoukian, "the threat to privacy arises not from the positive identification that biometrics provide, but the ability of third parties to access this in identifiable form and link it to other information, resulting in

---

[98] *Supra*, note 33, p.7.
[99] *Ibid*., p.7.
[100] *Supra*, note 33, p.7.

secondary uses of that information, without the consent of the data subject. This erodes the personal control of an individual over the uses of his or her information."[101] Mallon adds that

> The true privacy problems arise from third-party use of …technology. The biggest concern stemming from third party use is the potential for private citizens to develop and maintain vast amounts of information on individuals…. the fact that technology is giving private individuals power to recall personal information with a simple photograph raises concerns over the need to regulate this new technology. Without restriction, there is the potential for private use of face recognition technology (and other biometrics) to cross the boundary from providing security to invading privacy.[102]

There are two problems which impact privacy that are illuminated here. The first deals with the lack of accountability and potential for abuse by government and the private sector that operate these technologies; and the second pertains to the overarching need for regulation and legislation to define the parameters in which these groups should operate. Both of these will be discussed here briefly.

Feldman suggests that the "individual's interest in ensuring the accuracy and proper use of personal biometric information is unlikely to be fully represented by other actors in the system."[103] Agre asserts that "the potential for abuse is astronomical. Pervasive automatic face recognition could be used to track individuals wherever they go. Systems operated by different organizations could easily be networked to co-operate in tracking an individual from place to place. This tracking information could

---

[101] *Supra*, note 61, p.1.
[102] *Supra*, note 35, p.8.
[103] *Supra*, note 1, p.10.

be used for many purposes…. even more insidiously, tracking information can be used to exert social control"[104]

In addition, claims by companies and government agencies that their databases contain only wanted criminals raise other issues. Agre states that "we have to trust your word that the only people whose images are stored in the databases are wanted criminals, and we have to trust your word that you throw away all images that fail to match the database."[105] Agre also suggests that they really have no idea whether all of the people in the database are criminals as the quality control over these databases is far from perfect. Finally, even if the only people in the database today are criminals, the forces pushing down a slippery slope of ever-expanding surveillance are nearly overwhelming.[106]

Some of the issues which do not appear to have been dealt with by governments include who is permitted to collect information and under what circumstances; who is permitted to have access to the information and under what conditions; how are individuals able to review their information and correct inaccuracies; what is the process for people to challenge false rejects or claims that their image matches one on the system; how are private sector organizations who operate these systems on behalf of governments to be controlled and forced to be accountable to the populace and respectful of the national privacy laws. These are just some of the issues that remain outstanding and require clarification through legislation.

"Technology can introduce significant social changes while escaping the "pattern of deliberation and review" that governs social change. The problem is that inattention to technological developments leads to an increased risk of unanticipated adverse

---

[104] *Supra*, note, 56, p.2.
[105] *Ibid*., p.5.
[106] *Supra*, note 56, p.5.

social outcomes."[107] These risks include loss of privacy, loss of governmental and private sector accountability, and eventually, loss of democratic participation as people withdraw from the overwhelming scrutiny.

It is noteworthy that "in contrast to laws that apply to government, there have historically been far fewer common law or legislative restraints on industry information gathering practices…common law doctrine and statutory regimes have historically offered fewer protections against private sector data collection in part because non-governmental surveillance …does not appear to erode democratic values.[108] While the justification for the collection of this data has traditionally been defended as necessary in order to improve sales and marketing to customers, there is currently limited regulatory guidance to specify what information can be collected or whether these companies are prevented from sharing or selling those biometric records to others. This creates the danger of unscrupulous individuals or unethical companies accessing the personal information over which they have custody, in a nefarious manner that lends itself to fraud, identity theft, or "function-creep," which occurs when personal information is used for a purpose not originally intended.[109]

The unanimous consensus among commentators is that while the biometrics industry is attempting to create guidelines in order to self-regulate, "advocates of both privacy and facial recognition technology believe that there are too many dangers associated with these self-imposed guidelines, such as fraud and other illegal uses of the technology."[110] Further, both groups agree that

---

[107] *Supra*, note 86, p.8.
[108] *Ibid*., p.8.
[109] *Supra*, note 67, p.6.
[110] *Supra*, note 33, p.5.

legislation is required to prevent misuse of the technology by governmental agencies, corporations, or private citizens.[111]

According to McCoy, "the solution to the debate between privacy and the need for adequate and effective security measures can be resolved with appropriate legislation."[112] Further, "it is imperative that legislation defines the scope broadly enough to ensure the technology can be used effectively, but not so broad as to trample upon reasonable expectations of privacy."[113] The position is that detailed legislation will impact both law enforcement and citizens positively by creating a broad scope for the implementation of biometric technology while providing a focus on safeguarding privacy.[114]

Finally, it is important to acknowledge the fact that biometric technology is still developmental and evolving, and that "regardless of how much we invest in establishing standards for reliability of the technology and protections of the data from fraud or improper use, no system will be fool proof. Biometric determinations will be subject to mistakes, fraud, and abuse through human and technological error, both intentional and inadvertent."[115]

In addition, Mallon asserts that

> Recent studies have indicated a rather large percentage of error in the new technology. The National Institute of Standards and Technology…recently conducted a study to measure the accuracy of face recognition systems. According to the results, posed photos of a person taken only eighteen months apart, were rejected by the system,

---

[111] *Ibid*., p.5.
[112] *Supra*, note 33, p.8.
[113] *Ibid*., p.8.
[114] *Supra*, note 33, p.9.

[115] *Supra*, note 1, p. 2.

> which indicated no match approximately forty-three percent of the time. An anticipated DOD study is expected to confirm these statistics.[116]

A recent article confirmed additional technology failures during two separate tests conducted by the American Civil Liberties Union ("ACLU") and a Japanese research group from the University of Yokohama. The ACLU test discovered that facial recognition technology failed to match the faces with the names of 503 out of 958 volunteers, while the Japanese group discovered that fingerprints taken from drinking glasses could be replicated by jelly moulds, circumventing the effectiveness of fingerprint biometric technology.[117]

Lastly, Anthony Allan, Research Director with Gartner Research speaking at the European Biometrics Forum in Dublin stated that

> Even if sophisticated biometrics gear was in place in US airports, the technology alone probably would not have stopped the attacks. 'They were legitimate travellers,' referring to September 11th terrorists, 'they weren't known as terrorists then, so they wouldn't have appeared on recognition systems.' Indeed, Allan said that without adequate back security measures and databases, biometrics equipment is more or less useless…. biometrics has proven to be fallible, with evidence available that has shown that wearing glasses can fool an eye scanner, prosthetic make-up can affect face scanners, a sore throat can change a voiceprint and that breathing heavily on a fingerprint scanner can also make prints unrecognizable."[118]

---

[116] *Supra*, note 35, p.2.
[117] IT Law Today, '*Biometrics Don't Work: Says Research Reports*,' 2002, Online: <http://web.lexis-nexis.com/professional>. (Last accessed on 2 August 2004).
[118] The Register, '*Snags Hold Up Biometrics, Experts Say*,' by electricnews.net, 22n July 2003, Online: The Register,

During the same Forum, Kush Wadhwa, Director of Consulting from the International Biometrics Group, tried to dispel the notion that biometrics are the answer to world terrorism by asserting that "biometrics is a system like any other. Biometrics is one aspect, but one has to make sure all aspects of the system work."[119]

V. CONCLUSION

Biometric technology and its applications either offer tremendous opportunity in terms of increased security and safety, or a significant threat to privacy and the right to be free from unnecessary government intrusion into the daily affairs of the citizenry. The position one takes depends clearly on their viewpoint.

Proponents of this new technology believe that biometrics offer the definitive solution to the current maladies that afflict our societies: the on-going terrorist threat; social services and identity theft; fraud; border security; controlling asylum seekers, identifying illegal immigrants and eliminating anonymity from online transactions. These are all legitimate objectives.

However, the proponents urgency for a renewed sense of safety and security together with the blind adherence to all things scientific, have prevented this group from acknowledging two essential facts: first, biometric technology is under development and in the midst of an evolutionary process. It is not foolproof, remains untested in large, complex situations and has an enormous error rate. Reliance on unproven technology to solve such a wide array of problems without acknowledging the

---

<http://www.theregister.co.uk/2003/07/22/snags_hold_up_biometrics_experts/>, p.1.
(Last accessed on 9 August 2004).

[119] *Ibid*., p.2

technology's limits is dangerous, and in the case of the politicians who continue to pursue biometrics as the ultimate remedy, negligent.

Second, governments have historically had a difficult time using personal information contained in databases under their stewardship for only the purposes for which it was originally intended. As Matar points out, "history has shown us government officials have abused identification systems and databases in times of crisis…. government has a track record of using its authority to misuse the information with which it is provided in times of crisis. During such times, acts of illegal immigration, imminent threats of terrorism, and drug trafficking have trumped the importance of our basic civil liberties and privacy rights."[120]

Unfortunately, with biometric technology, this abuse may not be limited strictly to times of exigency, but could easily become a daily event, unbeknownst to the data subject. Government now has the option of utilizing the post September Eleventh reduced judicial scrutiny and relaxed legal requirements for monitoring individuals and increasing surveillance without any of the traditional privacy protections. Moreover, responses to privacy advocates concerns can now be dismissed by raising the "imminent terrorist threat" to quell objections to government activities which violate national privacy laws.

The threat to personal privacy extends beyond governments to their agents, private sector companies who are in the business of developing biometric technology or collecting, storing and maintaining personal information on behalf of their government contracts. These third parties are currently operating with limited legal legislation or regulations, and do not contend with the same legal restrictions which apply to government bodies. They are considerably dangerous to individual personal privacy and think nothing of sharing information with other organizations or selling

---

[120] *Supra*, note 49, p.10.

private data to other groups, under the pretence that the information belongs to them. Nuala O'Connor, Department of Homeland Security Privacy Officer, recently conceded that several American airlines had admitted to sharing massive amounts of passenger data with government contractors.[121] It is likely that this admission is only the tip of the iceberg.

It is imperative that governments develop privacy legislation and regulations that provide specific limits which define how biometric information is to be collected and used, by whom, and in what circumstances. Relying on existing legislation, which was drafted in a different time and under different conditions, when the application of biometric technology was not even a possibility, are not suitable for trying to curb the activities of governments and their agents in this new digital environment.

In addition, any anticipated legislation should provide clear procedures for enabling citizens to verify and correct information that pertains to them, and a process for challenging false rejects or false positives when an individual is wrongly denied access on the basis of a system error. Further, proposed legislation should also include significant penalties for any individual or group, that is determined to have inappropriately abused their fiduciary duty and either used, accessed, shared or sold personal information without the "unambiguous consent" of the individual. Until then, biometric technology will not reach its full potential but will instead become a tool of government social control aimed at the very people it was intended to protect.

---

[121] Wired News, '*Feds Seek Privacy Experts*,' by Joanna Glasner, 14 April 2004, Online: Wired News <http://www/wired.com/news/privacy/0,1848,63051,00.html>. (Last accessed 9 August 2004).

BIBLIOGRAPHY

JOURNAL ARTICLES

Agre, Philip E., 'Your Face is not Bar Code: Arguments Against Automatic Face Recognition in Public Places,' 2003, Online: <http://polaris.gseis.ucla.edu/pagre/bar-code.html>.

(Last accessed on 7 August 2004), 1-17.

Bharvada, Kamini, 'Electronic Signatures, Biometrics and PKI in the UK,' 2002, Int'l Rev. of Law Computers & Technology, 16(3), 265-275.

Cavoukian, Ann, 'Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look,' Informational and Privacy Commission for Ontario, (1998), Online: IPC, <http://www.ipc.on.ca/scripts/search>. (Last accessed on 7 August 2004).

Cockfield, Arthur, J., 'Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance,' 2003, 29 Queen's L.J., 364.

Davies, Simon, G., 'Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine,' 1994, Information, Technology and People, 7(4), 38-47.

Edwardson, Richard, 'National Identification Systems and Privacy Rights,' 2002, UCLA J. L. & Tech. Notes 4.

Electronic Frontier Foundation, 'Biometrics: Who's Watching You?,' Online: EFF <http://www.eff.org/privacy/surveillance/biometrics>. (Last accessed on 4 August 2004).

Feldman, Robin, 'Considerations on the Emerging Implementation of Biometric Technology,' 2003, 25 Hastings Comm. & Ent. L.J. 653.

Gates, Kelly A. 'Wanted Dead or Digitized: Facial Recognition Technology and Privacy,' 2002, Television and New Media, 3(2), 235-238.

House of Commons, Home Affairs Committee, 'Identity Cards,' Fourth Report of Session, 2003-2004, Vol.1, 20 July 2004, Online:

Home Office
<http://homeoffice.gov.uk/docs3/homeaffairs_idcards_30July.pdf>.
(Last accessed on 12 August 2004).

Klang, Mathias, 'Privacy Surveillance and Identity,' Chapter 14, From Book Pending Publication, 'Human Rights in the Digital Age,' Eds. Andrew Murray and Mathias Klang, (London: Glasshouse Press, 2004), Online: <http://www.digital-rights.net>.

Lyon, David, 'Surveillance After September 11,' 2001, Sociological Research, Online: <http://www.socresonline.org.uk/6/3/lyon.html>. (Last accessed on 5 August 2004).

Mallon, Bridget, ' "Every Breath You Take, Every Move You Make, I'll Be Watching You" The Use of Face Recognition Technology,' 2003, 48 Vill. L. Rev. 955.

Matsumoto, Tsutomu, et al., 'Impact of Artificial "Gummy" Fingers on Fingerprint Systems,' 2002, Prepared for Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 24-25 January 2002, Online:
<http://www.spie.org/Conferences/Programs/02/pw/confs/4677.html
>.

Matar, Neda, 'Are You Ready for a National ID Card? Perhaps We Don't Have to Choose Between Fear of Terrorism and Need for Privacy,' 2003, 17 Emory Int'l L. Rev. 287.

McCoy, Susan, 'O Big Brother, Where Art Thou? The Constitutional Use of Facial Recognition Technology,' 2002, 20 J. Marshall Computer & Info. L. 471.

Milone, Mark G., 'Biometric Surveillance: Searching For Identity,' 2001, 57 Bus. L. 497.

Nissenbaum, Helen, 'Privacy as Contextual Integrity,' 2004, 79 Wash. L. Rev. 119.

Tomko, George, 'Biometrics as a Privacy –Enhancing Technology: Friend or Foe of Privacy?,' Presented at the 'Privacy, Laws & Business 9th Privacy Commissioner's/Data Protection Authorities Workshop

1998, Online: <http://dss.state.ct.us/digital/tomko.htm>. (Last accessed on 3 August 2004).

Van der Ploeg, Irma, 'The Illegal Body: 'Eurodac' and the Politics of Biometric Identification,' 1999, Ethics and Information Technology, 1: 295-302.

Van der Ploeg, Irma, 'Biometrics and Privacy: A Note on the Politics of Theorizing Technology,' Information, Communication & Society, 2003, 6:1, 85-104.

Wong, Rebecca, 'Privacy: Charting It's Developments,' Chapter 12, From Book Pending Publication, 'Human Rights in the Digital Age,' Eds. Andrew Murray and Mathias Klang, (London: Glasshouse Press, 2004), Online: <http://www.digital-rights.net>.

LEGISLATION

Council Regulation (EC) No. 2725/2000 of 11 December 2000, Concerning the Establishment Of 'Eurodac' For the Comparison of Fingerprints for the Effective Application Of the Dublin Convention, 15.12.2000, Official Journal of the European Communities, Online: Europa

<http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_316/l_3162000/215en00010010.pdf>.

(Last accessed on 9 August 2004).

NEWSPAPER AND E-ARTICLES

BBC News, UK Edition, '*Health Tourism Rules Unveiled*,' 30 December 2003, Online: BBC <http://news.bbc.co.uk/1/hi/health/3355751.stm>.

(Last accessed on 14 August 2004).

BBC News, UK Edition, '*Tories Target 'Health Tourism'*,' 1 June, 2003, Online: BBC <http://news.bbc.co.uk/1/hi/uk_politics/2954438.stm>.

(Last accessed on 14 August 2004).

CBC, '*Indepth Screening: Airport and Border Security: National ID Cards*,' 2 April 2004, Online: CBC News Online <http://www.cbc.ca/printablestory.jsp>.

(Last accessed on 11 August 2004).

Globe and Mail, '*Biometric Identifiers Are on Way, Coderre Tells Group*,' by Campbell Clark, 9 October 2003, Online: Globe and Mail <http://www.theglobeandmail.com/servlet/ArticleNews/TPPrint/LAC/20031009/UIDENN/>.

(Last accessed on 11 August 2004).

IT Law Today, '*What is Biometrics*?,' March 2002, 10.2(27), Online: <http://web.lexis-nexis.com/professional/>.

(Last accessed on 2 August 2004).

IT Law Today, '*I Spy With Your Little Eye*,' August 2002, 10.6 (23), Online: <http://web.lexis-nexis.com/professional/>.

(Last accessed on 2 August 2004).

IT Law Today, '*Biometrics Don't Work: Says Research Report*,' 27 September 2002, 10.5(4), Online: <http://web.lexis-nexis.com/professional/>.

(Last accessed on 2 August 2004).

IT Law Today, '*Feeding the US Surveillance Monster*,' February 2003, 11.2(5), Online: <http://web.lexis-nexis.com/professional>.

(Last accessed on 2 August 2004).

Silicom.com, '*Compulsory ID Card Trial Scheme Launched*,' by Jo Best, 03 December 2003,

Online:http://management.silicon.com/government/0,39024677,39117190,00.htm>.

(Last accessed on 11 August 2004).

Silicom.com, '*ID Card "Route Map" Revealed by UK Passport Service*,' by Andy McCue, 31 March 2004, Online: <http://management.silicom.com/government/0,39024677,39119696,00.htm>.

(Last accessed on 11 August 2004).

Silicom.com, '*Blair: No ID Card Privacy Concerns*,' by Andy McCue, 02 April 2004, Online: <http://management.silicom.com/government/0,39024677,39119746,00.htm>.

(Last accessed on 7 August 2004).

Silicom.com, '*Biometric ID Card Bill on Its Way 'In a Month,*' by Jo Best, 8 April 2004, Online: <http://www.silicom.com/research/specialreports/protectingid/0,3800002220,39119896,00.htm>.

(Last accessed on 8 August 2004).

Silicom.com, '*Biometrics Are Key to UK ID Cards*,' by Will Sturgeon, 19 April 2004, Online: <http://software.silicom.com/security/0,39024655,39120070.00.htm>.

(Last accessed on 11 August 2004).

Silicom.com, '*Cheat Sheet: Biometrics*,' by Will Sturgeon, 20 April 2004, Online: <http://management.silicon.com/government/0,39024677,39120120,00.htm>.

(Last accessed on 8 August 2004).

Silicom.com, '*ID Cards: No Data Security Fears –and No Chance We'll Pay for Them*,' by Jo Best, 22 April 2004, Online:

<http://management.silicon.com/government/0,39024677,39120200,00.htm>.

(Last accessed on 8 August 2004).

Silicom.com, '*Biometric ID: 'Will Work, Will Happen, and Will Be Popular*,' by Will Sturgeon, 28 April 2004, Online: <http://software.silicon.com/security/0,39024655,39120303,00.htm>.

(Last accessed on 10 August 2004).

Silicom.com, '*Data Watchdog Blasts Secrecy Over ID Cards*,' by Jo Best, 09 June 2004, Online: <http://management.silicom.com/government/0,39024677,39121205,00.htm>.

(Last accessed on 11 August 2004).

Silicom.com, *'£35 Biometric ID Card Charge May Be Scrapped*,' by Andy McCue, 2 August 2004, Online: <http://management.silicom.com/government/0,39024677,39122805,00.htm>.

(Last accessed on 10 August 2004).

The Independent (London), 13, August 2003, '*Ever Feel You're Being Watched? Whether You're Traveling, Shopping, or on the Way to Work, Your Eyes Have It: Retinal Scanning is One of the New Biometric Systems Used to Check Identities.*' Online: <http://web.lexis-nexis.com/professional>.

(Last accessed on 7 August 2004).

The Register, '*Snags Hold Up Biometrics, Experts Say*,' by electricnews.net, 22 July 2003, Online: <http://www.theregister.co.uk/2003/07/22/snags_hold_up_Biometrics_experts/>.

(Last accessed on 9 August 2004).

The Register, '*Smart Cards, ID Cards, Nice, Nasty, Inevitable?*,' by John Lettice, 4 August 2003, Online: <http://www.theregister.co.uk/2003/08/04/smart_cards_id_cards_nice>.

(Last accessed on 9 August 2004).

The Register, '*Passport Biometric Trials Point Way for ID Cards*,' by John Leyden, 27 August 2003, Online: <http://www.theregister.co.uk/2003/08/27/passport_biometric_trials_point_way/>.

(Last accessed on 9 August 2004).

The Register, '*UK ID Card Plan –Intro Voluntary, Morph to Compulsory*,' by John Lettice, 6 November 2003, Online: <http://www.theregister.co.uk/2003/11/06/uk_id_card_plan_intro/>.

(Last accessed on 9 August 2004).

The Register, '*Data Watchdog Slams ID Card Plans*,' by John Leyden, 16 August 2004, Online: <http://www.theregister.co.uk/2004/08/16/id_cards_surveillance_fears/>.

(Last accessed on 18 August 2004).

The Times (London), '*A Threat to Liberty or a Threat to Terrorists?*,' by Danny Lee, 23 March 2004, Online: <http://web.lexis-nexis.com/professional/print>.

(Last accessed on 10 August 2004).

Wired News, '*Reporters Scowl at Face Scanners*,' by Declan McCullagh, 9 August 2001, Online: <http://www.wired.com/news/politics/0,1283,45950,00.html>.

(Last accessed on 08 August 2004).

Wired News, '*Feds Seek Privacy Experts*,' by Joanna Glasner, 14 April 2004, Online: Wired News <http://www.wired.com/news/privacy/0,1848,63051,00.html>.

(Last accessed on 9 August 2004).

Wired News, '*Biometric IDs Ok With U.K.*,' by Matthew Schwartz, 30 April 2004, Online: Wired News <http://www.wired.com/news/politics/0,1283,63282,00.html>.

(Last accessed on 9 August 2004).

WEBSITES

Canada Passport Office, '*Biometrics*,' Online: <http://www.ppt.gc.ca/faq/index/_e.asp#700>.

(Last accessed on 8 August 2004).

Canadian Internet Policy and Public Interest Clinic ("CIPPIC"), '*National ID Cards*,' Online: <http://www.cippic.ca/en/faqs-resources/national-id-cards/>.

(Last accessed on 10 August 2004).

CNN.com/US, '*Bush Vows to Rid World of 'Evil Doers*,' by Manuel Perez-Rivas, 16 September 2001, Online: CNN <http://www.cnn.com/2001/US/09/16/gen.bush.terrorism/>.

(Last accessed on 19 August 2004).

Europa – '*Eurodac*,' Official Journal of the European Communities, Online: <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_31620001215en00010010.pdf>.

(Last accessed on 7 August 2004).

House of Commons, Home Affairs Committee, '*Identity Cards*,' Fourth Report of Session 2003-2004, Volume 1, Report Together with Formal Minutes, Online: <http://homeoffice.gov.uk/docs3/homeaffairs_idcards_30July.pdf>.

(Last accessed on 11 August 2004).

Information and Privacy Commission/Ontario, Online: <http://www.ipc.on.ca/scripts/search/>.

(Last accessed on 7 August 2004).

PoliceOne.com, '*Big Brother Always Watching in Britain, Where Surveillance Cameras Are King*,' by Jane Wardell, **The Associated Press**, 13 August 2004, Online: PoliceOne.com <http://www.policeone.com/policeone/frontend/parser.cfm>.

(Last accessed on 18 August 2004).

UK Home Office, '*National Identity Cards*,' Online:

<http://www.homeoffice.gov.uk/comrace/identitycards/>.

(Last accessed on 8 August 2004).

UK Home Office, '*Identity Cards: 'The Next Steps*,' 2003, Online: <http://homeoffice.gov.uk/docs2/identity_cards_nextsteps.03111.pdf>.

(Last accessed on 8 August 2004).

Viisage – <http://www/viisage.com/ww/en/pub/home.cfm>.

(Last accessed on 12 August 2004).

Viisage, 'FaceFINDER,' Online: <http://www.viisage.com/ww/en/pub/viisage_products/facefinder/viisage_products_>.

(Last accessed on 12 August 2004).

Viisage, 'Identity Solutions' - <http://www.viisage.com/shared/data/pdf/identity_solutions.pdf>.

(Last accessed on 12 August 2004).

Welfare Watch, '*Welfare Reform: At What Human Cost?: Ontario Social Safety NetWork*,' Online:

<http://www.welfarewatch.toronto.on.ca/wrkfrw/humanco.htm.>.

(Last accessed on 18 August 2004).