

# 4 Biometrics and Privacy



In recent years, Biometrics technology has increasingly been used as a tool to improve security, and as a means to combat terrorism. But Biometrics, more so than any other type of technology, greatly impacts personal privacy. When deployed correctly, it can protect privacy; but when abused, or more commonly, when used without careful consideration, it can also lead to tremendous loss of privacy. This in turn erodes trust and engenders a climate of fear: the very thing terrorists hope to create. Is Biometrics compatible with Privacy? Some people would argue no. But perhaps a more practical approach is to explore ways to strike a balance. This article suggests five areas to consider: in Government, Industry, Education, Research, and International Cooperation. The real aim of this article is to create greater awareness of the issues involved, so that Biometrics does not inexorably lead to a Big Brother state.

**Dr Terence Sim**

School of Computing, National University of Singapore  
Chairman, Cross-Jurisdictional and Societal Aspects of Biometrics  
Working Group of Biometric Technical Committee (BTC)

### 1 Introduction

I have a nightmare that must be peculiar to my job as a professional in the area of Biometrics and Privacy. It goes like this:

My wife and I were returning from a holiday in Phuket, Thailand, when we were detained by Immigration Officers at Changi Airport. The Officers separated us and took me into a room for solo interrogation by one very eager Inspector.

Poh: Hello Mr. Sim. My name is I.M.K. Poh. I'm an inspector at the Police Cybercrime Unit. Welcome back from Bangkok.

Me: *Bangkok? I went to Phuket. I think you got the wrong person.*

Poh: Phuket? Yes, that's after Bangkok right? 6 days in Phuket, 1 night in Bangkok. (Starts to sing: ...one night in bangkok makes a hard man humble...)

*Me: Cut the song. Who told you?*

Poh: We work with the Thai Biometrics Dept. They have cameras all over the city, and look, their face recognition system spotted you in Patpong, with an unidentified topless female.

*Me: What?? Lemme see (I was shown a picture of me sitting next to a gorilla). This is ridiculous! That's somebody in a Gorilla costume, promoting Gorilla beer.*

Poh: Yeah, right. Who's ever heard of a beer named after an animal?

*Me: Tiger?*

Poh: Uh... never mind. That's not the reason I asked you here.

*Me: So why am I here?*

Poh: I have some good news and some bad news. The bad news: while you were away, someone stole your fingerprint and bought lots of things with it.

*Me: Oh my! No wonder I suddenly received so many spam SMS while in Thailand.*

Poh: Yes, we found out when the thief tried to buy a Bentley in your name. The car dealer got suspicious because, ahem, given your salary, you cannot afford the car. So the dealer called us. We checked with Immigration, and the Thai authorities, and knew you were out of the country. So this must be a case of identity theft.

*Me: So you arrested the thief?*

Poh: Well, sort of. He was found dead in your house.

*Me: What!? This is a nightmare! I need to sit down.*

Poh: The NEA<sup>1</sup> received complaints of mosquitoes coming out of your house. Since you were in Thailand until the weekend, they decided to enter the house to check. That's when they found the thief. Dead. From mosquito bites. He was still wearing a fake thumbprint to impersonate you. Apparently he was waiting for the Bentley to be delivered, but didn't expect the mozzies.

*Me: I... I don't know what to say. I feel faint.*

Poh: Well, the good news is, the NEA has cleaned your house very thoroughly. No more mozzies! Ever! They also want to thank you for the opportunity to photograph all the mosquitoes. They can now recognise every single insect from the way they fly. Anyway, everything is fine now. I just wanted to tell you... Mr Sim, Mr Sim? Are you okay? (Picks up phone) Hello, Medic? Come quickly. One guy just passed out...

<sup>1</sup> National Environment Agency: guardian of our environment; enemy of dengue.



## 2 What Went Wrong?

Hopefully, my nightmare never comes to pass; but it does highlight a number of grave problems that could happen if we are not careful about protecting privacy in this age of Infocomm Technology.

- Identity Theft: Stolen (fingerprint) biometric was used to make purchases under someone else's name.
- Function Creep: Use of data beyond what they were originally collected for. In this case, the data captured from my retail purchases I made were cross-referenced with my phone number to send spam SMS.
- Unauthorised Disclosure: How did the car dealer know my salary? How did NEA learn the date of my return? Obviously, the parties involved are revealing personal information without the owner's consent or knowledge.
- Invasion of Privacy: My movements from Phuket to Bangkok were monitored, my face was photographed, and such information was shared across geographical borders.

It is clear that the sharing of personal data, while sometimes increases one's convenience in obtaining services, can also invade one's privacy. In the coming years, the Singapore Government is embarking on a number of grand plans to boost the economy, create jobs, and improve living standards. There is the Intelligent Nation 2015, the National Authentication Infrastructure, the Infocomm Security Masterplan, and the Nationwide Micro-payment Platform (CEPAS), to name a few. These national efforts will no doubt transform the way we live and do business, and give us the needed competitive edge in an increasingly global village that we call Planet Earth.

Public concern for personal and data privacy has also gained momentum in recent years, with the Government responding by forming an inter-ministerial committee to review the need for a data protection law. This is a good sign - evidence that Singaporeans are more assertive of their personal rights, and that our Government is more attentive to the 'higher order' needs<sup>2</sup> of its citizens - especially as technology becomes more intrusive. In this regard, there is a new trend that, although somewhat abated since 11 September 2001, is quietly making inroads into our everyday life. I am referring to Biometrics, the technology that identifies people from their bodily traits (such as fingerprint patterns, iris scans, and face images).

In recent years, Biometrics is increasingly being deployed by the Government and private organisations. The main impetus for doing so is the threat of terrorism, and thus the need for better methods of personnel authentication as a way to prevent, or at least, deter terrorism. The purported superiority of Biometrics over traditional means of authentication, such as tokens and passwords, makes this new technology particularly attractive. However, without denigrating its usefulness, I would caution against the rapid and, often, blind adoption of a technology that has enormous implications on personal privacy. My nightmare is an example of how things could go wrong. Perhaps now that terrorism is not at red-alert levels we can take time to consider the impact of Biometrics on Privacy, before the next bomb explosion forces us to scan everyone everywhere.

To be fair, Biometrics did not engender privacy problems. Neither did Infocomm Technology. That dubious honor goes to human greed. But Biometrics aggravates these problems because of its unique ability to identify, and

<sup>2</sup> In terms of Maslow's Hierarchy. See [http://en.wikipedia.org/wiki/Maslow's\\_hierarchy\\_of\\_needs](http://en.wikipedia.org/wiki/Maslow's_hierarchy_of_needs), or [Maslow 1943].

hence track, every person uniquely. What can be done? I suggest five areas in which to channel our efforts. Some of these 'solutions', if I may call them such, are usually covered by data protection laws. However, Biometrics has its own peculiarities that must be specifically addressed. The five areas are: Government, Industry, Education, Research, and International Cooperation.

### 3 Government

The Government has two roles to play in making Biometrics safe for Privacy. It can pass new legislation to define the boundaries within which Biometrics (and other technologies) must operate. More effective would be to create a Privacy Commissioner to oversee and enforce the relevant laws. This is the route taken by countries such as Australia, Canada and Hong Kong. Table 1 shows the privacy legislations in a few countries. Interestingly, by comparing the second and last columns, it appears that having a Privacy Act does not depend on prior provision in one's Constitution, and vice versa.

Country	Privacy provided for in Constitution	Some related laws	Privacy Act?	Privacy Commissioner?
Singapore	No	Computer Misuse Act, Banking Act	No	No
China	Limited	Civil law, Practising Physician law	No	No
Hong Kong	in Basic Law	Consumer Credit Data Code	Personal Data (Privacy) Ordinance	Yes
United States	Not explicitly	USA Patriot Act	Limited to govt.	No
Australia	No	Crimes Act	Yes	Yes
Canada	Not explicitly	Personal Information and Electronic Documents Act	Yes	Yes

Table 1: Privacy legislation in selected countries. Data excerpted from [EPIC 2003]

There are many reasons why some countries have such laws while others do not. Mostly these have to do with the way each country has developed politically and economically. A significant reason also lies in the citizens' perception of its government. For example, Singaporeans are on the whole less suspicious of their Government than Americans. Hence they do not scrutinise the authorities for privacy violations as much as the Americans. Another example: Europeans tend to put more trust in their public officials than in private organisations; whereas for Americans it is just the opposite. Thus the European Union Data Protection Directive generally provides greater latitude for governments to collect and use personal data than for private companies to do the same. In contrast, Americans are more concerned about their Government becoming Big Brother than in the peccadilloes of private firms. Increasingly, however, each country is realising that new legislation is needed to cope with new issues (and new ways of perpetrating crime) brought about by technology. And the Universal Crime, for the moment, appears to be Terrorism.



The second, but not less important role the Government has to play is in self-regulation. The Government is by far the single largest deployer of Biometrics, and is likely to remain so even if more private firms adopt the technology. This is true in most countries. Think of the new passports that incorporate fingerprint and facial features, or of our National Identification Cards. How the Government polices itself in terms of protecting individual privacy drums the beat for others to march to.

Consider the widespread use of video surveillance cameras on the roads and in public places: the Government would do well to protect these images with suitable encryption and security mechanisms, as well as to regulate how its agencies use and share such data. For example, the Land Transport Authority, which analyses vehicular movements to monitor traffic condition, should not use the same videos to spy on an individual's driving habits, nor release them to the Ministry of Education for the latter to determine how school children spend their time after class. Of course, in the event of a national crisis, such cross-agency sharing may be necessary for the safety of the country, but these situations should be the exception and not the norm. More importantly, the Government needs to explain to its citizens how it safeguards such videos. This will not only increase public trust, but also set the gold standard for surveillance usage and disclosure everywhere.

The use of surveillance cameras, especially when combined with face recognition technology, raises a privacy issue peculiar to Biometrics, and not usually in the purview of data protection laws. Because a face image can be acquired from afar, without the subject's cooperation or even knowledge, the question is whether the individual should be informed that he is being photographed. Privacy advocates would say yes, he should be told. Moreover, if the individual objects to the act and chooses to leave the monitored area, then the captured images should be immediately deleted from the system. If, instead he chooses to stay, then his face images should be subject to the usual data protection laws.

In practice, such a position would be hard to defend. What if the monitored area is a public place, rather than the lobby of a private building? Does an individual have the right to expect personal privacy in a public space? Or what if the person has no choice but to use the monitored area because it is the only route to his destination? Does his continued presence imply consent to being photographed? On the other hand, suppose I set up a camera in my room so that it faces the street outside my window, and I broadcast the captured images on the Web. If you walked by and objected to my activity, what recourse do you have?

#### 4 Industry

Complementing government legislation, and often faster to enact, is a set of industry regulations developed and updated by a non-partisan Biometrics Association. Such an Association should ideally consist of vendors, users, legal counsellors, and academics. Its role is to promote best practices, certify compliance of vendor products with international Biometrics standards, educate the public, and otherwise regulate the industry. An example of this is the Biometrics Institute in Australia [Biomet 2001], which recently drafted a Privacy Code for the approval of the Australian Privacy Commissioner. The code recommends guidelines for how Biometrics data should be collected, used and disclosed, among other things, in order to protect personal privacy.

In Singapore, we currently have the Biometric Technical Committee (BTC), part of the IT Standards Committee [BTC 2001], and in which I am privileged to chair the Workgroup on Cross-Jurisdictional and Societal Aspects of Biometrics. The main role of the BTC is to participate in the international standards body on Biometrics, called

the ISO/IEC JTC1 SC37, and to recommend appropriate guidelines for Singapore. Our focus is thus towards setting standards rather than regulating the industry. As such, there is still a need for an independent, vendor-neutral Biometrics Association.

## 5 Education

There is as much hyperbole as myths concerning the supposed benefits, and ills, of Biometrics. Vendors tend to over-claim what their products can do, while the public is easily misled by Hollywood stereotyping of the horrors of technology. Both extremes are bad, and needs to be corrected by greater public education. For example, one common misconception is that the different types (modalities) of Biometrics can be ranked by how accurate they are, and therefore one should only choose the most accurate modality for maximum security. The truth is that there is no single notion of accuracy. Furthermore, Biometrics modalities are better assessed in terms of other criteria, not just accuracy<sup>3</sup>. No single modality is equally good across all these criteria. Therefore there is no such thing as the 'best' type of Biometrics, only what is appropriate for a particular application.

Besides misconceptions, there are also public prejudices that sometimes have to be overcome. Among older Singaporeans, for example, a common perception is that fingerprint acquisition is necessary only for criminals, or the illiterate. The educated and law-abiding citizen should therefore be exempted from such a demeaning practice.

The public also needs to be aware of their legal rights and their recourse in case of privacy violations. Question: Who is to pay for such education? Answer: The Government, since it is the dominant deployer of Biometrics. But perhaps a more practical answer is to share the burden among the Government, vendors, users, and concerned citizens.

## 6 Research

Since Biometrics is a technology, can its evils be curbed with more technology? In some cases, yes. It is possible to devise so-called Privacy-Preserving Technology. Such technologies protect privacy while enabling their benefits to be enjoyed. Scientists, recognising their role as responsible citizens, and wishing to contribute to the proper usage of their creations, have begun to research this area. One possibility centers around the problem of authorisation without identification.

Consider the common problem every organisation faces to grant its employees entry to their offices but to keep out non-staff members. The old way is to give each employee a key to his office. The Biometrics way is to control access using, say, fingerprints. However, this creates a problem that the humble low-tech key avoided: it is now possible to determine not just who is allowed to enter, but who actually entered. That is, the old way only permitted an authorised **group** of people to access the room, but does not pinpoint which **individual** actually entered. This is authorisation without identification. The high-tech way, unfortunately, both authorises and identifies. Worse, when coupled with the time of entry and exit, such information could be used to penalise an employee for not spending enough time in the office.

One technological solution to this problem of separating identification from authorisation relies on something called Zero-Knowledge Proof [Gold 1985]. The idea is for me to convince you, via a series of questions and answers,

<sup>3</sup> A commonly-used set of criteria include Universality, Uniqueness, Permanence, Collectability, Performance, Acceptability, and Circumvention. See [Yau 2003] for more details.



that I know a secret without actually revealing it to you. If I succeed in doing so, you can be (almost 100%) certain that I have knowledge of the secret, but you would still not know what that secret is. And if that secret is my identity, then I would have assured you of my authorisation without revealing who I am. This may sound bizarre, but a simple analogy aptly illustrates the idea<sup>4</sup>.

A popular series of book puzzles in the late 1980s was one called Where's Waldo? (or Where's Wally?), created by Martin Handford [Waldo 1987]. The objective is to locate Waldo, a bespectacled man wearing a striped-shirt, in a large crowd of people wearing similar attire. Suppose I wish to convince you that I know where Waldo is on a particular page of the book. If I simply pointed him out, you would know that I know where Waldo is, but you would also know his location. However, if I covered the page with a large sheet of paper, and cut a hole just big enough to reveal Waldo, but not his surroundings, then I would have proven to you that I know Waldo's location, but you would still be ignorant!

It should be clear how such technologies inherently limit the type of knowledge transferred between parties, and can therefore be used to directly protect privacy. In contrast, legal regulations work indirectly, by deterring, rather than preventing, privacy abuse. Research in Privacy-Preserving Technology should therefore be encouraged and funded.

## 7 International Cooperation

As with fighting terrorism, privacy issues require cooperation across national borders. Referring again to my nightmare, the information provided by the Thai authorities enabled the Singapore side to act swiftly and decisively. In this hypothetical scenario, neither country respected my privacy. It should be obvious that mutually equivalent privacy laws and practices have to be in place for both countries to benefit. If one country has 'weaker' laws and lax practices, then an individual's personal information can be abused when it flows over there. Given the worldwide trend to outsource routine work (and hence data) to countries with equivalent skills but cheaper wages, this issue of cross-border privacy compatibility becomes a serious one.

It is therefore understandable why, in trade negotiations, larger, dominant countries pressure their smaller trade partners to enact comparable laws. Anyone signing a Free-Trade Agreement with the US knows this. Interestingly, in 2000, the Americans were themselves pressured by the Europeans to tighten their privacy laws before trans-Atlantic data flow would be permitted. This resulted in the Safe Harbor Agreement [Safe 2000].

## 8 Conclusion

Terrorism is a real threat. When an attack happens, people are willing to give up some personal privacy for national security. This is just Maslow's theory in action. Yet when the threat subsides, people do not usually regain the privacy rights they surrendered. This sort of asymmetry bothers Privacy Advocates. Another asymmetry lies in the (unfortunate) fact that certain groups of the population are subject to greater scrutiny and less privacy than others. The poorer citizens, or the minority race, or criminals (even after they have reformed) tend to form this group. There are no easy solutions to the balance of Biometrics and Privacy. In this article, I have merely suggested some ideas, but raised more questions in the process. As an academic, I consider it my job to create awareness and to ask questions. And perhaps to share my nightmares.

<sup>4</sup> This analogy is due to [Naor 1999].

## 9 References

- [Biomet 2001] Biometrics Institute.  
[www.biometricsinstitute.org](http://www.biometricsinstitute.org)
- [BTC 2001] Biometrics Technical Committee.  
[www.itsc.org.sg/tc/tc.html](http://www.itsc.org.sg/tc/tc.html)
- [Epic 2003] Electronic Privacy Information Centre. Privacy and Human Rights 2003.
- [Gold 1985] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems. Proceedings of 17th Symposium on the Theory of Computation, Providence, Rhode Island. 1985.
- [Maslow 1943] Abraham Maslow. A Theory of Human Motivation. Psychological Review, Vol. 50, NO. 4, p. 370-396, 1943.
- [Naor 1999] Moni Naor, Yael Naor, and Omer Reingold. Applied Kid Cryptography, 1999.  
[www.wisdom.weizmann.ac.il/~naor/PUZZLES/waldo.html](http://www.wisdom.weizmann.ac.il/~naor/PUZZLES/waldo.html)
- [Safe 2000] The Safe Harbor Agreement. U.S. Department of Commerce.  
[www.export.gov/safeharbor/index.html](http://www.export.gov/safeharbor/index.html)
- [Waldo 1987] Where's Waldo? Martin Hanford. Candlewick, 1987.
- [Yau 2002] Yau Wei Yun. The '123' of Biometric Technology. Synthesis Journal 2002.

