IS MALAYSIA'S MYKAD THE 'ONE CARD TO RULE THEM ALL'? THE URGENT NEED TO DEVELOP A PROPER LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL INFORMATION IN MALAYSIA

MATHEWS THOMAS*

[In September 2001, the Malaysian government officially launched a multipurpose smart identification card for its citizens. This card, named 'MyKad', incorporates multiple applications with several sets of personal information about the holder of the card. Given the scope of the applications and the extensive personal information that is and can be stored in the MyKad, the implementation of the MyKad project raises crucial issues about information privacy and the protection of the personal information of Malaysians. This article critically examines these issues and contends that the existing legal framework does not adequately protect personal information. As such, there is an urgent need for the development of a proper legal framework to address the far-reaching information privacy implications arising from the project. The author argues that to ensure greater protection of personal information in Malaysia and to better regulate the collection and use of personal information on the MyKad, there is a need for both strong personal data protection legislation and judicial recognition of a right to information privacy as a fundamental human right guaranteed by the Malaysian Constitution.]

CONTENTS

I Introduction 475
II The MyKad 476
A Background 476
B Technical Operation 479
C Information Content and Applications 481
III Information Privacy Implications of the MyKad 484
A Information Privacy and the Protection of Personal Information 484
B 'Authorised' Use of Personal Information by the Government 485
1 Data Surveillance 485
2 Discrimination 486
3 Function Creep 487
C Unauthorised Use of Personal Information 488
1 Misuse through Corruption 488
2 Error or Incompetence 490
3 Theft by Third Parties 490
D Incorrect Personal Information 491
E The Government's Response 491

* BA (ANU), LLB (UNSW), LLM (Monash); Lecturer, School of Business, Monash University (Malaysia). This article is based on the author's research undertaken in relation to a research paper submitted in May 2003 towards fulfilment of the requirements for the Master of Laws degree at Monash University. The author wishes to thank Dr Elizabeth Lanyon, the then Director of Postgraduate Studies, Faculty of Law, Monash University, for her valuable suggestions and comments on the issues discussed in this article. The author also wishes to express his gratitude to the two independent referees who made constructive and positive comments on several parts of this article.

IV Existing Legal Framework 492
A Statutory Framework 492
B Common Law Position 495
C Some Observations 497
V The Personal Data Protection Bill 498
A Background to the Personal Data Protection Bill 498
B Scope of Protection 498
C Data Matching 500
D Exemptions 502
E Independence of the Commissioner 503
F A Case for Reform 504
VI A Constitutional Right to Information Privacy 505
A Information Privacy as a Human Right 505
B The Malaysian Constitution and the Court of Appeal 505
C The Indian Experience 507
D A Constitutional Right 509
VII Conclusion 510

I INTRODUCTION

In Malaysia, the national identity card system has been operational since 1949[1] — even before Malaysia attained independence from British colonial rule. In September 2001, the Malaysian government officially launched a multipurpose smart identification card for its citizens.[2] This smart card, named 'MyKad',[3] incorporates in a single card multiple applications with several sets of personal information about the holder of the card.[4]

The MyKad is the world's first government-backed smart card initiative and it has been heralded as a giant step in information technology both in Malaysia and worldwide. However, given the scope of the applications and the types of personal information contained in the MyKad, the implementation of the MyKad project[5] raises crucial issues about the privacy and protection of the personal information of Malaysians. These issues are the subject matter of this article.

Part II begins with an outline of the background, technical operation and information content of the MyKad. Part III examines the information privacy implications arising from the extensive personal information that is and can be stored in the MyKad as well as the potential for misuse of such personal infor-

1 Patsy Kam, 'A Card for All Reasons', *The Star* (Malaysia), 13 December 2001, Section 2, 3.

2 National Registration Department, Malaysia, *Government Multipurpose Card Project Special Report* (2001) 39, 47.

3 'My' in MyKad signifies personal ownership as well as Malaysia's domain name. 'Kad' is the acronym for both 'Kad Akuan Diri' (Personal Identification Card) and 'Kad Aplikasi Digital' (Digital Application Card): National Registration Department, Malaysia, *MyKad*: *The Government Multipurpose Card* <http://www.jpn.gov.my/gmpc/GMPC.htm>.

4 This information includes personal identification, driving licence details, passport information, health information and an electronic purse cash balance: see below Part II(C).

5 For the purposes of this article, references to 'the MyKad project' encompass the multipurpose card, all the supporting infrastructure, including software and hardware, and the network of databases in connection with implementation of the applications and functions of the card. References to 'the MyKad' signify the multipurpose card itself, unless the context indicates otherwise.

mation by the government or other parties. In view of these implications, Part IV considers the existing legal framework in Malaysia and highlights inherent deficiencies in the extent of the current protection of personal information. This author argues that as a result of these deficiencies, there is an urgent need for the development of a proper legal framework to address the far-reaching information privacy implications arising from the implementation of the MyKad project.

Part V evaluates the personal data protection legislation drafted by the government. The author identifies some of its major shortcomings and suggests several measures to make the proposed legislation a viable mechanism for protecting the personal information stored in the MyKad. In addition, and more importantly, the author argues in Part VI for the recognition, through judicial activism, of a right to information privacy as a fundamental human right guaranteed by the *Malaysian Constitution*.

Thus this author argues that the extent, collection and use of the personal information stored in the MyKad may be better regulated by placing the protection of information privacy on a constitutional footing and by strengthening the proposed personal data protection legislation. This would ensure greater protection of personal information in Malaysia.

II THE MYKAD

A *Background*

In line with Malaysia's 'Vision 2020', which is to achieve developed nation status by the year 2020,[6] the Multimedia Super Corridor ('MSC') was established in 1996.[7] The MyKad project is one of seven flagship applications of the MSC.[8] It is in fact the brainchild of the then Prime Minister, Dr Mahathir, who intended to amalgamate the multiple existing cards with different purposes into a single card incorporating all the pertinent information about each Malaysian citizen.[9]

The National Registration Department ('NRD') is the lead government agency for the MyKad project and is supported by other government departments.[10] A

[6] Development is not merely infrastructure and technology; it is, in essence, the development of human resources without which there would be no long-lasting economic progress. For a discussion of the definition of a 'fully developed country', see Mahathir Mohamad, 'The Way Forward' (Speech delivered to the Malaysian Business Council, Kuala Lumpur, 28 February 1991) <http://www.pmo.gov.my/website/webdb.nsf/vALLDOC/BA7051FF90767AD848256E84003129CA>.

[7] See generally Multimedia Development Corporation, *The Multimedia Super Corridor* (2003) <http://www.msc.com.my/msc/msc.asp>; Abu Bakar Munir, *Cyber Law*: *Policies and Challenges* (1999) 33–4.

[8] These applications, which also include electronic government and smart school initiatives, are to slingshot Malaysia into being a cyber-savvy producer, exporter and user of computer technology by the year 2020: see Multimedia Development Corporation, *About the Flagship Applications* (2003) <http://www.msc.com.my/msc/flagship.asp>.

[9] Kam, above n 1.

[10] The other major government departments are the Road Transport Department, the Royal Malaysian Police, the Immigration Department and the Ministry of Health. There was an initial rejection of the MyKad initiative by some of these government agencies due to intergovernmental rivalry resulting from the lead role taken by the NRD and due to a lack of information or

consortium of five companies, each specialising in a different area, is involved in the production, implementation and problem-solving aspects of the MyKad project.[11]

The MyKad project has been developed at a cost of RM276 million.[12] At 5 May 2004, approximately 9.9 million cards had been issued,[13] with another nine million Malaysians above the age of 12 planned to carry the card by the end of 2005.[14]

To date the MyKad has been widely accepted by the people of Malaysia and has been generally uncontroversial. This is partly because both before and since independence, Malaysians from the age of 12 have had to carry a national identity card. Thus, there has been no uproar from the public such as was seen in Australia when the Hawke government attempted to introduce the Australia Card in the late 1980s.[15] If anything, the general response in Malaysia has been one of

understanding on the part of these agencies. When the MyKad was first launched and used as a driving licence, the Road Transport Department issued a summons against a MyKad holder for not having a valid driving licence, refusing to accept his MyKad as such: K Saithuruka, 'Stop Rejecting MyKad, Says NRD: New Information Card a Valid Document, Agencies Told', *The Star* (Malaysia), 3 November 2001, 6. The Director-General of the NRD, Azizan Ayob, has said that 'the NRD should be the lead agency because we are the custodians of personal details and MyKad is a security matter involving highly sensitive documentation and information': Mary Anne Tan, 'Net Value: Digitising Our Identity', *The Edge Daily* (Malaysia), 14 January 2003 <http://www.theedgedaily.com/cms/content.jsp?id=com.tms.cms.article.Article_18679>. These government departments work in conjunction with the Multimedia Development Corporation ('MDC'), which has the overall task of implementing the MSC: see generally Multimedia Development Corporation, *The Multimedia Super Corridor*, above n 7.

11 The five companies are: Unisys (M) Sdn Bhd, which is responsible for the overall systems integration and project management; Iris Technologies Sdn Bhd, which is in charge of the chip operating system and its multi-level security features; Dibena Sdn Bhd, which physically prints the card and personalises it by printing the individual's information on the card; Computer Systems Advisors ('CSA') Malaysia Bhd, which supplies the device interface and designs the infrastructure for the network that connects the various government agencies to the card functions; and ENCPR Sdn Bhd, which develops and supplies the Card Acceptance Devices and biometric devices: see Rina Omar, 'MyKad Has It All', *New Straits Times* (Malaysia), 29 March 2002, Talk Zone 3; Multimedia Development Corporation, *One Card System* (October 2002) <http://www.msc.com.my/today/html/20021029_mscgen_001.asp>.

12 Tan, above n 10. It is uncertain whether this figure is an accurate one, since a similar project in Hong Kong was valued at US$392.36 million (RM1.49 billion) in 2002. See Trade Media Holdings Ltd, *Hong Kong to Roll Out Smart ID Card System for All Residents by 2003* (2002) Global Sources <http://www.globalsources.com/MAGAZINE/SECURITY/0208/SMART.HTM>.

13 Multimedia Development Corporation, *Flagship Applications — Progress Status* (2004) <http://www.msc.com.my/flagship.asp>. The number of cards issued as at July 2003 stood at 5.7 million: M Krishnamoorthy, 'MyKad Under-Utilised', *The Star Online* (Malaysia), 10 July 2003 <http://www.thestar.com.my/services/printerfriendly.asp?file=/2003/7/10/nation/5811392.asp>. The applications in the MyKad, such as the electronic purse and automatic teller machine ('ATM') access, nevertheless remain under-utilised: 'Malaysia's National Smart Card Under-Used', *CNETAsia* (Singapore) 11 July 2003 <http://www.asia.cnet.com/newstech/systems/0,39001153,39139994,00.htm>.

14 Jane Ritikos, 'New MyKad Deadline and Fine', *The Star* (Malaysia), 7 April 2004, 3. For future consolidation of the MyKad project, all babies born from March 2003 will be issued with the 'MyKid', a derivative of the MyKad: 'MyKid for All Newborn Babies Soon', *The Star* (Malaysia), 26 February 2003, 15. The MyKid, according to the government, will facilitate a child's dealings with school registration, hospitalisation and banking. Conversion to the MyKad will take place when the child reaches the age of 12: National Registration Department, Malaysia, *MyKid* <http://www.jpn.gov.my/mykid.htm>.

15 Simon Davies, *Campaigns of Opposition to ID Card Schemes*, Privacy International <http://www.privacyinternational.org/issues/idcard/campaigns.html>.

mild enthusiasm about having to neither carry multiple forms of identification nor pay an application fee, which has been waived until December 2005.[16]

However, some members of the public, members of the opposition in Parliament and public interest groups have raised concerns about privacy risks and have criticised the lack of public consultation about the MyKad.[17] This author has observed that these criticisms have not received sufficient attention from the government-friendly media in Malaysia, although they have been reported more fully in the non-mainstream newspapers and online news portals.[18] Notwithstanding these general criticisms, there has not been any systematic or detailed analysis of the MyKad project from a legal or privacy perspective since its launch. This is most likely due partially to a lack of awareness of the privacy issues underpinning the MyKad and partially to the limited amount of publicly available information about the MyKad project that is independent of the government.[19]

[16] See 'MyKad for All Malaysians by 2005, Says PM', *The Star* (Malaysia), 21 September 2002, 4; 'Bajet 2003: Komen Orang Ramai', *Utusan Malaysia* (Malaysia), 21 September 2002, 11. Dr Mahathir announced this waiver when tabling the 2003 Budget at the Second Reading of the Supply Bill 2003: Malaysia, *Parliamentary Debates*, House of Representatives, 20 September 2002, IV(34), 25 (Mahathir Mohamad, Prime Minister).

[17] Teresa Kok, Member of Parliament for Seputeh, has strongly criticised proposals to include marital status and voting constituency information in the MyKad: Teresa Kok, 'The Government Is Urged to Seriously Review the Inclusion of the Information of Marital Status and Voting Constituency on MyKad' (Press Release, 27 September 2002) <http://www.malaysia.net/dap/bul1752.htm>. Members of the public have given a mixed response to the inclusion of marital status: Audrey Edwards, 'MyKad Inclusion of Marital Status Causes Some Ripples', *Sunday Star* (Malaysia), 22 September 2002, 6. The Consumers' Association of Penang ('CAP') has argued that the MyKad renders individuals' personal and confidential information open to abuse: ' "Smart IC" Open to Abuse, Says CAP', *The Star* (Malaysia), 18 April 2001, 10. The Federation of Malaysian Consumers Association ('FOMCA') has been reported in the mainstream media as being concerned about privacy intrusion: Kam, above n 1. In addition, FOMCA has criticised the government for not implementing clear guidelines or consulting with the public on how, by whom and for what purpose the MyKad is to be used and has contended that the storage of personal information in a centralised database makes it vulnerable to tampering: Electronic Privacy Information Center, *Privacy and Human Rights 2003*: *An International Survey of Privacy Laws and Developments* (2003) <http://www.privacyinternational.org/survey/phr2003/countries/malaysia.htm>. See also the general criticisms raised by two advocates and solicitors: Kean Chye Lim, 'MyKad: Invasion of Privacy' (2003) 32(3) *Insaf*: *The Journal of the Malaysian Bar* 91; Samirah Muzaffar, 'Privacy and Security: The Smart Card Conundrum' [2004] 2 *Malayan Law Journal* lix. For a more humorous (and still accurate) critique of the MyKad, see TV Smith, *TV Smith's Dua Sen*: *The Naked Card* (2003) <http://www.mycen.com.my/duasen/150703_mykad.html>.

[18] See the concerns expressed by several individuals about privacy implications of the MyKad in *Malaysiakini*, a non-mainstream news portal: Jeffrey, 'Dangers Lurk in MyKad', *Malaysiakini*, 23 September 2002 <http://www.malaysiakini.com/letters/24109>; Khairul Khalifah, 'Digital IDs Open to Abuse', *Malaysiakini*, 24 September 2002 <http://www.malaysiakini.com/letters/24117>; Citizen Cane, 'Why We Should Say "No" to MyKad', *Malaysiakini*, 27 September 2002 <http://www.malaysiakini.com/letters/24138>; Belkisa Lim, 'Who Has Access to Personal Information in MyKad?', *Malaysiakini*, 11 July 2003 <http://www.malaysiakini.com/letters/25669>; AAR, 'MyKad Has Extreme Social Impact on Citizens', *Malaysiakini*, 14 July 2003 <http://www.malaysiakini.com/letters/25681>.

[19] In writing this article, this author is somewhat limited by this second constraint. This is a particular problem in terms of the security and privacy protection and other measures that have or ought to have been implemented within the framework of the MyKad system. To this extent, the analysis in this article is based on the limited technological information about the MyKad that is publicly available and it may therefore not represent a comprehensive evaluation of all the privacy issues arising from the implementation of the MyKad project.

B *Technical Operation*

The MyKad is similar in size to a credit card. Its computer chip enables numerous functions in the MyKad, including data processing, file management and the storage of large amounts of information.[20]

The MyKad is secured by both physical card features[21] and chip security features.[22] The Chip Operating System ('COS') enables control over the read and write access to data on the MyKad.[23] There is also a firewall or security function that constrains the access of different government agencies to the information relevant to their line of duty.[24]

The chip is designed to be used at Government Service Centres ('GSCs')[25] and accessed by Card Acceptance Devices, including key ring readers.[26] The GSCs' main functions are to input, process and update information on the MyKad as well as to process applications for new MyKads.[27] The GSCs also communicate with the cardholders' central database, which is located at the headquarters of the NRD.[28] The central database is maintained by the GSC back-end server, which also serves as a gateway to agency host computers and financial institutions.[29]

The desktop CADs enable authorised access at the GSCs, at selected government agencies and at certain other locations, such as private hospitals.[30] Gov-

[20] Intel Corporation, *MyKad*: *Challenge* (2004) <http://www.intel.com/cd/business/enterprise/apac/eng/bss/products/casestudies/84342.htm>. The original computer chip has now been superseded by one with greater memory (64KB) to enable more applications than were previously available: 'MyKad for Online Dealings', *The Star* (Malaysia), 14 February 2003, 4.

[21] These include 'micro lettering; guilloche patterns; relief pattern; latent text; rainbow printing; ultraviolet image … and holographic overlay': Intel Corporation, *MyKad*: *Solution* (2004) <http://www.intel.com/cd/business/enterprise/apac/eng/bss/products/casestudies/84398.htm>.

[22] The chip itself is secured via encryption and authentication, including through thumbprint biometrics which dispense with the need for a Personal Identification Number ('PIN') as a form of authentication: see ibid; Omar, above n 11.

[23] See Iris Corporation Berhad, *OS for Smart Card Microprocessor Chips* (2002) <http://www.iris.com.my/Technology/tec_os.asp>.

[24] See Omar, above n 11; below nn 31–2, 35 and accompanying text.

[25] The GSCs are 'the front-line one stop services [sic] centres for all MyKad related transactions to the public'. There are 13 GSCs at present around the country. They feature workstations, digital cameras, biometrics scanners to record fingerprints and desktop Card Acceptance Devices ('CADs'): Intel Corporation, *Mykad*: *Solution*, above n 21.

[26] See generally ibid. The CADs are card readers that have been developed to access, retrieve and, in some instances, write information in the MyKad in a secure manner. There are four main CADs: desktop CADs used at the GSCs, mobile CADs used by enforcement agencies, immigration autogates used at immigration exit and entry points and key ring readers, which are smaller devices that have limited access and read functions: National Registration Department, Malaysia, *MyKad*: *The Government Multipurpose Card*, above n 3; see below nn 30–3 and accompanying text.

[27] See generally ibid; Multimedia Development Corporation, *One Card System*, above n 11.

[28] Intel Corporation, *Mykad*: *Solution*, above n 21.

[29] See ibid. There is insufficient publicly available information as to how this central database is maintained. A network probably connects the various government agencies that maintain separate databases, each holding a different type of information, to the functions of the MyKad: Multimedia Development Corporation, *One Card System*, above n 11.

[30] These CADs allow for specific information to be uploaded onto or downloaded from the MyKad or the relevant database: Multimedia Development Corporation, *One Card System*, above n 11; Intel Corporation, *Mykad*: *Solution*, above n 21.

ernment enforcement agencies including the NRD, the Road Transport Department, the Immigration Department and the Royal Malaysian Police, as well as paramedics, have mobile CADs which can read, access, write, print and utilise specific information on the MyKad, and which can also upload and download blacklists and summons data from the respective databases.[31] Some of these enforcement agencies also have key ring readers which allow for read-only access to specific types of information on the MyKad.[32] The key ring readers and various versions of the CADs with limited access rights or the ability to access the 'open information' embedded in the MyKad[33] are available for sale to the public and to private sector organisations for applications such as the 'Visitor Management System' and the 'Hospital Information System'.[34]

As a result of the security features and technological specifications of the MyKad and its supporting infrastructure, specific types of personal information in the MyKad and in the respective databases can be accessed by certain government agencies or selected third parties who have the appropriate access rights.[35] However, it is uncertain how and by whom access rights are determined. Both the level of access granted or enabled through the CADs and the purpose for which these access rights may be exercised are similarly unclear. There are no statutory provisions in the *National Registration Act 1959* (M'sia) ('*NRA*') or the *National Registration Regulations 1990* (M'sia) ('the Regula-

[31] Intel Corporation, *Mykad*: *Solution*, above n 21. A summons can be issued in respect of traffic offences committed under the *Road Transport Act 1987* (M'sia) ('*RTA*'). A motorist who pleads guilty to the offence will be imposed with a prescribed fine or, in the case of an offence that may be compounded, a compound: see *RTA* ss 119(4), 120(1). The Road Transport Department and Royal Malaysian Police have a 'blacklist' of motorists with outstanding summonses or unpaid fines or compounds: see Road Transport Department of Malaysia, *Blacklist Inquiry* (2004) <http://www.jpj.gov.my/blacklist/index.shtml>.

[32] Key ring readers are small devices attached to a key ring holder. Personalised key ring readers which allow an individual to read only the text-based data or 'open information' embedded in the MyKad can be purchased by the public: National Registration Department, Malaysia, *MyKad*: *The Government Multipurpose Card*, above n 3. Any person with a key ring reader can read the open information on the MyKad. However, the electronic purse cash balance in the MyKad can only be read by the MyKad holder if the key ring reader is specially designed to do so: see, eg, Iris Corporation Bhd, *MyKad Info at Your Fingertips* (Brochure) <http://www.iris.com.my/product/pdf/KRR112.pdf>.

[33] The 'open information' embedded in the MyKad includes the name, identification number, residential address, age, gender, race and driving licence details of the MyKad holder, as well as a 'Y' (for 'yes') or 'N' (for 'no') code for prior criminal record or restricted residence. This open information was viewed by the author when testing a CAD available for sale to the public.

[34] The Visitor Management System is an application marketed by ACA Pacific Technology (M) Sdn Bhd which uses the CADs developed by Iris Corporation Berhad 'to access, retrieve, print and use the information stored in the chip that is embedded in [the] MyKad' in order to maintain a log of all visitors to any organisation and track their entry into and exit from the building: ACA Pacific Technology (M) Sdn Bhd, *Visitor Management System* (2003) <http://www.acapacific.com.my/article.php?sid=175>. The Hospital Information System is another such application. It uses CADs to retrieve a patient's information from the MyKad and to track their every step from appointment bookings through to clinical sessions, drug dispensation and final billing: ACA Pacific Technology (M) Sdn Bhd, *Accurate Fast Data Retrieval; Reduce Human Errors; Improve Customer Services — with Smart Card Applications* (Brochure).

[35] These rights can be granted through the issue of a PIN to the relevant authorised officer, which must be keyed into the CAD to allow access to or changing of the personal information in a MyKad: Kam, above n 1.

tions')[36] setting out restrictions on the types of information that may be accessed from the MyKad or the respective databases by any particular category of authorised officers.[37] Any grants of access rights to the various authorities and third parties have thus far been done administratively and without transparency or public disclosure.

The NRD, as the agency maintaining the central database for the MyKad project, and other enforcement agencies such as the Royal Malaysian Police and the Anti-Corruption Agency, may already have, or be able to obtain, access rights to *all* types of personal information in the MyKad. In any event, certain government agencies and third parties will have access to all the open information about the MyKad holder embedded in the MyKad.

C *Information Content and Applications*

While the MyKad was originally intended to contain four applications —the national identity card, driving licence, passport information and health information — it now incorporates eight applications, with the possibility of additional applications being integrated in the future. The other four applications are the electronic purse, ATM access, transit application (the 'Touch 'n' Go' feature) and the Public Key Infrastructure ('PKI') feature for online transactions.[38] In the near future the government intends to merge the MyKad with the Payment Multi-Purpose Card ('PMPC'),[39] which will enable the MyKad to have debit and credit card functions and other financial applications.

The MyKad replaces the existing paper-based laminated national identity card as well as the driving licence. It displays on its surface most of the information currently printed on the existing national identity card, driving licence and passport.[40] However, pursuant to recent amendments to sch 1A to the Regulations,[41] additional personal information can be displayed on the card's surface and stored in the chip. Consequently, the cardholder's gender and religion (if the holder is Muslim) are now displayed on the MyKad surface. The chip contains information including: race and religion (for all), thumbprints,[42] polling station code and date of registration as a voter, code for criminal record and restricted residence, driving summons or compound[43] and demerit points and health information.

36 Unless otherwise stated, all references to regulations in this article are references to these Regulations.

37 See below Part IV.

38 See Multimedia Development Corporation, *Multi-Purpose Card* (2003) MSC Expo 2003 <http://www.msc-expo.com.my/home.htm>; see below nn 49–51 and accompanying text.

39 Li Za Wong, 'Wise Up to Role of Smart Card', *Sunday Star* (Malaysia), 15 December 2002, 25.

40 These include: an identification number; name; residential address; residential or citizenship status; driver's licence class, number and type; passport number, type and expiry date; and the holder's photograph.

41 *National Registration (Amendment) Regulations 2001* (M'sia).

42 The surface of the existing national identity card has the left and right thumbprint impressions of the holder.

43 If summonses are issued for traffic offences that may be compounded, a fixed sum or fine can be collected from the person reasonably suspected of having committed the offence: see *RTA*

Apart from personal identification and driving licence information, the MyKad also complements the Malaysian international passport for exit from and re-entry into Malaysia, although the passport is still required for entry into and exit from foreign countries. It was originally announced that Malaysians travelling to Brunei would be allowed to use the MyKad in lieu of a passport,[44] but according to the NRD Director-General, Wan Ibrahim Wan Ahmad, this development has been delayed due to a need to protect the personal information in the MyKad when the card is used as a travel document.[45] Health information in the MyKad includes blood group, any allergies, implants, long term illnesses, medical prescriptions and dosage, and records of the holder's last two ward admissions or clinical visits and diagnoses (if any).[46] In addition, while he was Prime Minister, Dr Mahathir announced the inclusion of additional information on marital status[47] and voting constituency.[48] This announcement indicates that the nature and categories of personal information that can be stored in the MyKad in the future are not closed.

The electronic purse application in the MyKad facilitates payment for small purchases and can be used for commercial transactions and transactions with government agencies (which until now have required the cumbersome process of obtaining bank drafts or money orders). The ATM access application allows storage of up to three bank accounts in the MyKad and enables MyKad users to carry out common banking activities, such as cash withdrawals, balance inquiries and transfers of funds.[49] As part of the transit application, the 'Touch 'n' Go' feature facilitates payment of bus and light rail transportation fares and parking fees, as well as payments at toll booths and at other outlets which accept this payment system.[50] The PKI application in the MyKad provides security for online transactions as well as the transmission of information over networks

s 120(1). In such instances, the offender pays the compound and there is no prosecution of the traffic offence.

44 Sa'odah Elias and Sim Leoi Leoi, 'To Brunei with MyKad: Indonesia, Thailand May Be Next to Have Passport-Free Travel', *The Star* (Malaysia), 18 December 2003, 2.

45 'Technical Problems Delay Use of MyKad as Passport', *The Star* (Malaysia), 23 June 2004, 12.

46 Sch 1A to the Regulations.

47 Malaysia, *Parliamentary Debates*, House of Representatives, 20 September 2002, IV(34), 25. His rationale for the inclusion of marital status is that 'the enforcement authority will not mistakenly apprehend people for close proximity'. 'Close proximity' or 'khalwat' refers to the offence where unmarried Muslims are found in compromising situations or close proximity without a lawful basis. There have been instances where Muslim married couples have been wrongly apprehended by the religious authorities: Kok, above n 17.

48 Malaysia, *Parliamentary Debates*, House of Representatives, 20 September 2002, IV(34), 25. The inclusion of voting constituency will, according to Dr Mahathir, mean that 'certain parties will not be able to transfer voters'. This statement alludes to the government's contention that opposition parties had transferred voters in the 1999 elections in their bid to win in marginal constituencies: Sa'odah Elias, 'Power to Transfer: Move to Allow Polls Panel to Clean Up Roll of Phantom Voters', *The Star* (Malaysia), 15 March 2003, 1. This allegation is one that the opposition parties usually level at the ruling National Front party: Anil Netto, 'A New Era Begins' (2000) 20(9) *Aliran Monthly* 2, 6. It must be noted that at present the two categories of information (marital status and voting constituency) are yet to be incorporated into sch 1A to the Regulations.

49 Multimedia Development Corporation, *Multi-Purpose Card*, above n 38; National Registration Department, Malaysia, *MyKad*: *ATM* (Brochure).

50 Multimedia Development Corporation, *Multi-Purpose Card*, above n 38.

because public-key cryptography allows for the use of digital signatures and therefore for the authentication of identity.[51]

Proposed applications include Employee Provident Fund (superannuation) transactions,[52] voter registration, ticketless air travel and car park access.[53] The MyKad is also now used by organisations to control the access of visitors and employees to secured areas,[54] for work scheduling and for the internal flow of information and operations within these organisations.[55] As indicated by Dr Mahathir, the possibilities for usage of the MyKad are immense and '[t]he journey into the digital era has not just ended with th[e] launch [of the MyKad], rather; this is the beginning of a new era of civilization.'[56]

At present, the MyKad is optional for Malaysians except where they have lost or damaged their existing paper-based identity cards[57] or are applying for an identity card for the first time.[58] Administratively, however, the NRD has ceased to issue the existing paper-based identity cards since 31 July 2001.[59] Thus, there is effectively no option — all Malaysians will at some stage have to change to the MyKad.[60]

The MyKad therefore represents, on the one hand, a single smart card that can be used for multiple purposes and which the government promises will propel Malaysians towards 'an incredible transformation in their lives'.[61] On the other hand, the MyKad contains, in one card, considerable personal and potentially sensitive information about the cardholder. It also has considerable capacity for expansion into other domains. As a result, serious information privacy issues must be urgently addressed.

51 Ibid.

52 The Employee Provident Fund is a statutory scheme established under s 24(1) of the *Employees Provident Fund Act 1991* (M'sia) which provides for retirement benefits of all private sector and non-pensionable public sector employees: see Employees Provident Fund, *Corporate Profile*: *Mission* <http://www.kwsp.gov.my/index.php?ch=91&pg=182&ac=1197&lang=eng>. All employees who are covered by this legislation and their employers are required to make monthly contributions to the fund: *Employees Provident Fund Act 1991* (M'sia) s 43(1).

53 Center for Digital Government, *MyKad*: *The Malaysian Government Multipurpose Card* (2003) Government Technology International <http://www.centerdigitalgov.com/international/story.php?docid=49229>.

54 Multimedia Development Corporation, *MyKad Introduces New Feature — Access Control* (2003) MSC Today <http://www.mdc.com.my/today/html/2003-Feature_030710_01.asp>; Elan Perumal, 'NRD to Implement MyKad Entry System', *The Star* (Malaysia), 8 July 2003, 20. For a discussion of the Visitor Management System, see above n 34 and accompanying text.

55 Mimos Bhd, 'Mimos Is First with MyKad Integration for Corporate Use' (Press Release, 9 July 2003) <http://www.mimos.my/clear/press_mykad.htm>.

56 Center for Digital Government, above n 53.

57 Regulation 13.

58 Saithuruka, above n 10.

59 Omar, above n 11.

60 Indeed, the Minister of Home Affairs, Datuk Azmi Khalid, will seek Cabinet approval for a deadline requiring all Malaysians to switch to the MyKad by mid-2006: Embun Majid and Jane Ritikos, 'MyKad Deadline Mulled: Holders of Old IC Must Switch by 2006, Says Azmi', *The Star* (Malaysia), 9 August 2004, 3.

61 Multimedia Development Corporation, *One Card System*, above n 11.

III INFORMATION PRIVACY IMPLICATIONS OF THE MYKAD

A *Information Privacy and the Protection of Personal Information*

The concept of 'privacy' has been the subject of dispute and discussion by many scholars, jurists and judges over the years. At a very general level, the right to privacy involves the 'right to be let alone.'[62] It is beyond the scope of this article to delve into the debate surrounding the definition of privacy or its many connotations and dimensions. Four (slightly overlapping) privacy interests are commonly identified,[63] but this article focuses only on information privacy.

As a starting point, this article adopts a definition of 'information privacy' as 'the interests of an individual in controlling the information held by others about that person'.[64] The right to information privacy involves the protection of personal information against misuse. The term 'personal information' is used in this article, adopting Raymond Wacks' proposed definition, as involving

> those facts [or data], communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation.[65]

With the tremendous technological developments in the speed of collection, storage and transmission of personal information over computer networks and the internet, information privacy has become an area of great international concern. The MyKad raises similar concerns about information privacy because the one card brings together a comprehensive personal dossier from different sources relating to an individual.[66] Through the PIN given to each MyKad

62 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 195, citing Thomas Cooley, *A Treatise on the Law of Torts* (2nd ed, 1888) 29.

63 The four commonly identified privacy interests are: (a) information privacy — the interests of the individual in controlling the information held by others about that person; (b) territorial privacy — the interest in controlling intrusion into aspects of behaviour, particularly regarding sensitive issues; (c) bodily privacy — the interest in freedom from interference with one's physical person; and (d) communications privacy — the interest in freedom from surveillance and privacy of communications. See Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* (1999) Australian National University <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>; Mark Berthold and Raymond Wacks, *Hong Kong Data Privacy Law*: *Territorial Regulation in a Borderless World* (2nd ed, 2003) 4.

64 Berthold and Wacks, above n 63.

65 Raymond Wacks, *Personal Information*: *Privacy and the Law* (1989) 26; see also Raymond Wacks (ed), *Privacy*: *The Concept of Privacy* (1993) vol 1, xvi. This definition has been adopted to indicate the minimum level of personal information that requires urgent protection. It is somewhat more restrictive than the definition of 'personal information' used in various personal data protection and privacy Acts. For example, in Australia, s 6(1) of the *Privacy Act 1988* (Cth) defines 'personal information' as

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

See also the definition of 'personal data' in the draft Personal Data Protection Bill 1998 (M'sia): below n 146. These definitions do not feature the two restrictions — the intimacy of information and the individual's wish to withhold it — that are proposed by Wacks.

66 A similar sentiment has been expressed by the Hong Kong Privacy Commissioner for Personal Data in respect of the proposed Hong Kong Smart ID Card: Office of the Privacy Commissioner

holder, which can be used to access and retrieve all types of information about the individual if the user of the CADs has access rights to such information, the MyKad can be used to retrieve and consolidate information about an individual held in previously unconnected computer databases situated around the country. Moreover, this unique personal identifier can allow multiple government agencies or other third parties who can use CADs or GSCs to gain access to this consolidated information.

Hence, the nature and amount of personal information stored on the MyKad raises several serious concerns about the information privacy of Malaysians. Both authorised and unauthorised access to such personal information can result in its misuse. These concerns are examined below.

B *'Authorised' Use of Personal Information by the Government*

1 *Data Surveillance*

While some of the personal information on the MyKad is already contained on the existing national identity card, the additional types of personal information in the MyKad and the linking of that information through the PIN can facilitate data surveillance of an individual by the government and its enforcement agencies. This approach is reminiscent of the Orwellian concept of 'Big Brother', giving rise to major privacy concerns. As a leading English case anticipated:

> if the information obtained by the police, the Inland Revenue, the social security offices, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state.[67]

Data surveillance involves the systematic use of personal data systems in the investigation or monitoring of actions or communications of an individual or group of persons.[68] It can result in the use, albeit 'authorised', of personal information for purposes other than that for which the information was collected. Such surveillance could result in the personal information stored in the MyKad being used for secondary purposes, such as profiling certain categories of individuals or matching their personal data records to identify people of potential interest to the government. While this may empower enforcement agencies to create profiles on or to track suspected 'criminals', it will also enable the government to electronically monitor other individuals who are considered to be 'subversive', whether they are members of identified subversive groups, posing a security threat to the government, or simply critical of it.[69]

for Personal Data, Hong Kong, 'Privacy Commissioner for Personal Data Expresses Views on ID Card Schemes' (Press Release, 19 October 2000) <http://www.pco.org.hk/english/infocentre/press_20001019.html>.

67 *Marcel v Commissioner of Police of the Metropolis* [1992] Ch 225, 240 (Browne-Wilkinson VC).

68 Clarke, *Introduction to Dataveillance*, above n 63.

69 This can be carried out at several levels, including the tracking of movements into and out of Malaysia and the tracking of movements within Malaysia by monitoring payments at 'Touch 'n' Go' points and ATM transactions.

'Big Brother' surveillance is of particular concern due to the inclusion of highly sensitive personal information in the MyKad such as voting constituency and voter registration information. This type of information can enable the government to monitor individuals' voting patterns[70] and effectively interfere with or discourage voter turnout during national elections.[71] The inclusion of health information, such as any long-term illnesses, and of marital status, could also lead to the monitoring and surveillance of individuals or groups who may be of particular interest to the government due to their 'alternative' or 'non-conformist' lifestyles.

This capability for extensive data surveillance would confer on the government even greater power and control over its citizens, potentially giving the government detailed insight into the private lives of MyKad holders. As cautioned by a leading commentator on this issue: '[a]ll human behaviour would become transparent to the State, and the scope for non-conformism and dissent would be muted'.[72]

2 *Discrimination*

A related concern is that the extensive amount of personal information stored in the MyKad may encourage discriminatory practices by government agencies. Enforcement agencies are equipped with mobile CADs with radio frequency to read and access the MyKad and the respective databases.[73] Certain segments of the population may be targeted, harassed or victimised by these enforcement agencies[74] on the basis of the information in the MyKad relating to race,[75] religion, HIV status, past criminal record or marital status. These enforcement

[70] In order to vote, a registered voter must currently produce either the MyKad or the existing identity card at the registration counter in any polling station. The voter is then given a registration number that is matched to her or his unique PIN. Upon presentation of the registration number at the balloting room, a ballot with a serial number is given to the voter and the voter's registration number is noted against the counterfoil of the ballot which is retained by the Election Commission. This gives rise to the potential for the ballot to be eventually matched against the individual. While this potential has always existed, the use of the MyKad and the computerisation of the voter registration process has substantially increased the potential for monitoring, tracking and linking votes cast to voters.

[71] Voting is not mandatory in Malaysia. As it is, voter turnout has been on the decline in Malaysia in recent years: see International Institute for Democracy and Electoral Assistance, *Voter Turnout from 1945 to Date*: *A Global Report on Political Participation*: *Malaysia*, International IDEA Voter Turnout <http://www.idea.int/voter_turnout/asia/malaysia.html>. Although there is no evidence that the government has ever tracked individual votes under the traditional balloting system, the increased potential to do so now may act as a deterrent to voters, particularly civil servants: Electronic Privacy Information Center, *Privacy and Human Rights*, above n 17.

[72] Roger Clarke, 'Chip-Based ID: Promise and Peril' (Paper presented at the International Conference on Privacy, Montreal, 27 September 1997) <http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html>.

[73] See above n 31 and accompanying text.

[74] See generally Simon Davies, *Identity Cards*: *Frequently Asked Questions* (1996) Privacy International [10] <http://www.privacy.org/pi/activities/idcard/idcard_faq.html>.

[75] Group classifications in identification cards based on race or ethnic origins have been identified as playing a major role in facilitating crimes of genocide and ethnic cleansing, for example in Rwanda and Nazi Germany: Jim Fussell, 'Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing' (Paper presented at the Seminar Series of the Yale University Genocide Studies Program, Connecticut, 15 November 2001) <http://www.preventgenocide.org/prevent/removing-facilitating-factors/Idcards>.

agencies could gain access to the MyKad on the pretext of inquiring about something else and then treat the holder in a discriminatory manner based on the accessible information.

For example, in the employment context, the recording of marital status could result in discrimination against unmarried single mothers or divorcees.[76] Similarly, an individual from an opposition-controlled constituency could face unfair treatment or discrimination in terms of employment opportunities or promotion prospects within the civil service on the basis of the information in the MyKad pertaining to voting constituency.[77] Past criminal record and restricted residence recorded in 'Y' (for 'yes') or 'N' (for 'no') format are part of the open information embedded in the MyKad[78] and are accessible by any party or government agency that has a CAD or key ring reader. An individual who has a prior criminal record, irrespective of the nature of the offence, or who for whatever reason has restricted residence, may face discriminatory treatment not only in relation to employment opportunities or promotion prospects, but also when seeking entry into buildings or using services from government agencies or third parties.

3 *Function Creep*

Another concern arising from the 'authorised' use of personal information by the government is that of 'function creep',[79] whereby more and more functions and information are added to the MyKad over time. As mentioned above, the original four applications proposed for the MyKad have now been expanded to eight, with the possibility of additional applications.[80] The announcement concerning the inclusion of marital status and voting constituency in the MyKad is a clear example of function creep.[81] The government may be adopting the approach taken in Australia when the idea for the Australia Card was first introduced. In that context, the Health Insurance Commission stated:

> It will be important to minimize any adverse public reaction to implementation of the system. One possibility would be to use a staged approach for implementation, whereby only less sensitive data are held in the system initially with the facility to input additional data at a later stage when public acceptance may be forthcoming more readily.[82]

[76] Kok, above n 17. Kok states that there is considerable stigma attached to single unmarried mothers or divorcees in Malaysia.

[77] See ibid; Editorial, 'MyKad Will Bring You Multi Purpose Headaches!', *Ipoh-Online*, 2002 <http://www.ipoh-online.com.my/editorial/003.htm>.

[78] See above n 33.

[79] Davies, *Identity Cards*, above n 74, [11]; Office of the Privacy Commissioner for Personal Data Hong Kong, 'Privacy Must Be Protected with the New Smart ID Card' [2000] 5 *Private Thoughts*: *Newsletter of the Office of the Privacy Commissioner for Personal Data* <http://www.pco.org.hk/textonly/english/publications/newsletter_2000nov.html>.

[80] See above n 38 and accompanying text.

[81] See above nn 47–8 and accompanying text.

[82] Health Insurance Commission, *An Outline Plan Prepared for the Inter-Departmental Commmittee on National Identification* (1985) 4, cited in Roger Clarke, *Just Another Piece of Plastic for Your Wallet*: *The 'Australia Card' Scheme* (1987) Australian National University <http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html>.

It is probably only a matter of time before an individual's taxation and employment information will be incorporated into the MyKad to facilitate tax returns and the collection of income tax.

Private sector applications of the MyKad, such as controlling access to secured buildings and tracking visitors using the publicly available CADs,[83] give private sector organisations the capacity to electronically record and store the open information of individuals who visit these organisations. Such information could then be used by these private sector organisations for unrelated activities, such as offering to sell it for the purposes of marketing or direct selling.

The introduction of additional information and the increase in MyKad applications will broaden the number of government agencies and private sector organisations that have access to the personal information stored in the MyKad. There is a serious possibility that this will result in greater infringement of information privacy rights and widen the possibility of the misuse of personal information.

C *Unauthorised Use of Personal Information*

1 *Misuse through Corruption*

The MyKad project involves the five major solutions providers,[84] the MDC, the major government departments involved in the implementation of the MyKad, the enforcement authorities and other support agencies. Such a comprehensive project involves thousands of people within the public service as well as the private sector. This gives rise to a further privacy concern — the misuse of personal information through corruption. Private sector models cited in United Kingdom debates have 'generally assumed that at any one time, one per cent of staff will be willing to sell or trade confidential information for personal gain'.[85]

Malaysia is no stranger to corruption.[86] In Transparency International's Cor-

[83] See above nn 34, 54–5 and accompanying text.

[84] See above n 11 and accompanying text.

[85] Davies, *Identity Cards*, above n 74, [13]. A study concluded in New South Wales in 1992 revealed many privacy violations related to the abuse of personal information in records by information users inside and outside the government: Independent Commission against Corruption, *Report on Unauthorised Release of Government Information* (1992) vol 1, ix, 3.

[86] The issue of rampant police corruption in Malaysia was highlighted in Parliament pursuant to a 2001 Police Commission Report which indicated that each year at least 1000 police officers were disciplined for offences including bribery and corruption: Foo Yee Ping, Izatun Shari and Dalilah Ibrahim, 'Police Abuse Tarnishing Its Image, Says MP', *The Star* (Malaysia), 14 March 2003, 6. More recently, the Royal Commission on the Royal Malaysian Police presented its preliminary report to Malaysia's King and the Prime Minister. This report documents many complaints received by the Commission regarding rampant corruption at all levels of the police force: 'Graft a Problem in Force: Commission Hands over Report on Police to PM', *The Star* (Malaysia), 10 August 2004, 2. Despite calls from opposition leaders, the report of the Royal Commission has yet to be made public: see Kit Siang Lim, 'Cabinet Tomorrow Should Direct the Full and Immediate Public Release of the Royal Police Commission Interim Report to Demonstrate that the Government Is Serious about Accountability, Transparency, Good Governance and a World-Class Police Force to Roll Back the Crime Wave in the Country' (Press Release, 10 August 2004) <http://www.dapmalaysia.org/english/lks/aug04/lks3154.htm>; 'Govt Taking Steps to Weed Out Corrupt Cops', *The Star* (Malaysia), 11 August 2004, 4. In addition, the level of corrupt practices

ruption Perceptions Index 2002, the country received a score of 4.9, indicating the existence of a relatively high level of corruption.[87] Despite the infancy of the MyKad project, there are already allegations that illegal immigrants in Malaysia's eastern state of Sabah possess valid MyKads.[88] There have been instances of forgery and counterfeiting of existing identity cards and other high security devices — not due to a lack of security features, but due to the assistance of corrupt public officials holding positions of trust in government.[89]

The various types of personal information in the MyKad would be of great value to third parties for purposes ranging from marketing and direct selling to identity theft.[90] The fact that the security features of the MyKad would make it difficult for these parties to gain access to such information would in turn increase its value. This is likely to add to the temptation for public officials to engage in corrupt practices, including the unauthorised use or disclosure of the personal information in the MyKad. This could occur through the direct sale or disclosure of the personal information to third parties, the illegal sale or duplication of CADs or the unauthorised sale of access rights to third parties. Even a single incident of such corruption could severely jeopardise the information privacy of individual citizens.

Notwithstanding its high security features, the integrity and efficacy of the MyKad project depends on the trustworthiness of all the people involved in its implementation. This is an assurance that the Malaysian Government cannot yet give to its citizens.

among civil servants in Malaysia appears to be on the rise: Rais Yatim, Minister in the Prime Minister's Department in Simon Khoo, 'ACA Too Quiet, Says Rais', *The Star* (Malaysia), 19 May 2003, 10.

87 Transparency International, *Corruption Perceptions Index 2002* (2002) <http://www.transparency.org/pressreleases_archive/2002/2002.08.28.cpi.en.html>. The Corruption Perception Index score is out of a clean score of 10. The score obtained by Malaysia for the year 2002 is lower (more corrupt) than the score of 5.0 obtained in 2001 or the score of 5.32 obtained in 1996.

88 'Police Task Force to Investigate MyKad Allegations in Keningau, Wilfred to Bring the Matter Up in Parliament', *New Sabah Times* (Malaysia), 18 June 2002 <http://www.upko.org.my/arkibberita-jun02/tangau-mykad-180602.htm>. More recent reports from the state of Sabah indicate the continued existence of syndicates that prey on illegal immigrants attempting to acquire identity cards: 'IC "Dealers" Prey on the Gullible', *The Star* (Malaysia), 7 April 2004, 8.

89 Instances of forged MyKads held by illegal immigrants in the state of Sabah were raised by the Member of Parliament for Seputeh, Teresa Kok, at the committee stage during the debate on the motion to reduce the emoluments of the Deputy Minister of Home Affairs. During her speech, Kok highlighted instances of the misuse of personal identification numbers by the NRD of Sabah that resulted in the issuance of a number of identity cards in Sabah with the same identification numbers. She queried the Deputy Minister on the outcome of investigations into these matters: Malaysia, *Parliamentary Debates*, House of Representatives, 23 October 2002, IV(53), 125–6; see also 'Citizenship for Aliens, Govt Legalising Phantom Voters: DAP', *New Sabah Times* (Malaysia), 21 May 2003 <http://www.newsabahtimes.com.my/May2003/20.5/local4.htm>. The first arrest of a foreigner with a forged MyKad was made recently, where the counterfeit document had features like the genuine MyKad and was found to be a 'good forgery'. Investigations are ongoing: R S N Murali, 'Man with Fake MyKad Held: First Known Case since Its Introduction', *The Star* (Malaysia), 6 August 2004, 6.

90 Identity theft 'refer[s] to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain': United States Department of Justice, *Identity Theft and Fraud* (2000) <http://www.usdoj.gov/criminal/fraud/idtheft.html>.

2 *Error or Incompetence*

Another area of concern is that through incompetence, error or lack of adequate training on the part of the public officials or other parties entrusted with the implementation of the MyKad project, the personal information of cardholders may be inadvertently released to third parties. This may occur due to a jumbling of files or through the circulation of statistics in a form that reveals personal information about individuals.[91] While such inadvertent disclosure may have occurred prior to the MyKad regime, the nature and extent of the personal information stored in the MyKad would make the consequences of such disclosure more severe.

A further concern is that the NRD may erroneously issue an individual's MyKad to an unintended recipient.[92] Besides experiencing the inconvenience and difficulties of obtaining a new MyKad, the MyKad holder would face the risk of unauthorised use of his or her personal information as well as the risk of identity theft by unknown individuals.[93]

A related issue is that there is no culture of respect for information privacy within the government bureaucracy and enforcement agencies.[94] Without such respect or coherent training on the necessity of safeguarding the privacy of citizens, inadvertent disclosures of personal information and careless handling of the MyKad are likely to occur.

3 *Theft by Third Parties*

A further privacy vulnerability is the theft of personal information either via hackers or through other means. The MyKad system appears to be a prime target in this respect given the nature and amount of information in the MyKad and the tremendous value of obtaining personal information. Moreover, the networked structure of the databases increases the amount of information that can be obtained if the system is breached. In such a case, the information retrieved can easily be duplicated electronically. It would be almost impossible to obtain security sufficient to prevent such theft.[95]

[91] In the context of the introduction of computer systems, see Colin Tapper, *Computer Law* (3rd ed, 1983) 122.

[92] One such incident has already been reported. An applicant who went to collect his new MyKad from the NRD branch in Ipoh in December 2003 was informed that someone else had already collected the card. The applicant refused to reapply for the MyKad: 'Applicant Finds MyKad Missing: Man Claims Dept Gave His New IC Away', *The Star* (Malaysia), 24 April 2004, 25.

[93] See above n 90.

[94] The saga involving the arbitrary detention of foreign Indian information technology professionals in Kuala Lumpur and the defacing of their passports by members of the Royal Malaysian Police, purportedly to determine the genuineness of these passports, is symptomatic of this deficiency: see Chun Wai Wong, 'Probe on Claims of Indian IT Workers', *Sunday Star* (Malaysia), 16 March 2003, Comment 33.

[95] See generally Andrew Clement et al, *National Identification Schemes (NIDS) and the Fight against Terrorism* (2001) Computer Professionals for Social Responsibility <http://www.cpsr.org/program/natlID/natlIDfaq.html>.

D *Incorrect Personal Information*

The incorrect *collection* of personal information can also give rise to the invasion of an individual's privacy. In the event that inaccurate information is collected and stored on the MyKad or the database system, even the most law-abiding citizen may be subjected to scrutiny by law enforcement agencies. The networking of databases within the MyKad system would replicate these inaccuracies from one database to another, leading to decisions being made based on incomplete or inaccurate information about a particular individual. A system as expansive as the MyKad project is likely to contain a significant amount of incorrect personal information.

As a result of such inaccuracies, the MyKad holder may be victimised, harassed or subjected to data surveillance through no action of his or her own.[96] That individual may not even know about the inaccuracies until the damage is done.

E *The Government's Response*

To date, the Malaysian government has sought to reassure its citizens that their privacy will not be threatened by emphasising the high security features of the MyKad that are supposedly inviolable.[97] There has, however, been no proper examination of any of the information privacy concerns highlighted above nor any attempt to address these prior to or even during the implementation of the MyKad project. Ironically, the MyKad project director, Wan Mohamad Ariffin Wan Ismail, stated that:

> One of the main worries that the public has is security. But frankly, having additional information in your [MyKad] is no big deal and *doesn't compromise your privacy in any way*. The other fear is that Big Brother (the government) will constantly be keeping tabs on you. But consider this: military people have always carried a special ID and in no way has it impeded their freedom.[98]

Essentially, the Malaysian government does not consider that the extent of information in the MyKad compromises the information privacy of its citizens. This is probably because the right to information privacy is yet to be legally or even politically recognised by the government.

96 See generally ibid.

97 Wan Mohamad Ariffin Wan Ismail, the MyKad project director of the NRD, has assured MyKad holders that the biometric verification and other safety devices built into the MyKad will not allow other people to use their cards: cited in Kam, above n 1. See also above n 45 and accompanying text regarding the assurances by the NRD Director-General, Wan Ibrahim Wan Ahmad, that the delay in using the MyKad as a passport is related to security issues.

98 Quoted in Kam, above n 1 (emphasis added).

IV EXISTING LEGAL FRAMEWORK

A *Statutory Framework*

A number of statutes in Malaysia impact either directly or indirectly on the use and disclosure of the personal information stored in the MyKad. The primary statute that regulates the personal information stored in the MyKad is the *NRA*. Section 5 of the *NRA* requires every person in Malaysia for three months or more to be registered in accordance with the *NRA* and the Regulations. Through registration, each individual is issued with an identity card, such as the MyKad,[99] containing the particulars required by sch 1A to the Regulations.[100]

Personal information to be stored in the MyKad is recorded by a registration officer[101] prior to the issuance of the card. Under reg 13A of the Regulations, the particulars on a driving licence are also incorporated into the MyKad. This includes the particulars of any conviction or disqualification.[102]

Section 58(2) of the *RTA* requires any driver of a motor vehicle to produce his or her driving licence for inspection at the request of any police officer, traffic warden or road transport officer. If the driving licence is incorporated in the MyKad, this means that the MyKad must be produced for inspection. In addition, registration officers are empowered under reg 7(1) of the Regulations to ascertain the identity of any person by demanding the MyKad.[103] If an officer discovers that the MyKad is false or has reasonable cause to suspect that the information stored in the MyKad is false, then she or he is empowered, inter alia, to seize the MyKad and deliver it to the nearest registration office for investigation.[104]

The police have been issued with more than 1500 mobile CADs to check whether MyKad holders have outstanding summonses, have committed offences or are the subject of an arrest warrant.[105] Registration officers are similarly equipped. However, there do not seem to be any statutory restrictions at present in the *NRA* or *RTA* as to the types of information that may be accessed by these officers.

99 The MyKad falls within reg 2, which defines a 'Government multi-purpose card' as 'an electronic card embedded with an electronic microchip capable of storing and processing a person's personal particulars for the functions and applications prescribed by the Director General from time to time [and which] includes a high security identity card with chip.'

100 See above nn 41–2, 46 and accompanying text.

101 A registration officer is defined to include the Director-General of the NRD, registration officers and registration agents (who are not public officers) appointed by the Director-General, and any road transport officer, immigration officer or any officer of any government department who is appointed by the Director-General as a registration officer: *NRA* ss 2, 3B. Registration officers are regarded as public servants for the purposes of the *Penal Code* (M'sia) ('*Penal Code*'): *NRA* s 3C.

102 Regulation 13A read together with *RTA* ss 34 and 34A (not yet in force).

103 This regulation also empowers any police officer, customs officer or member of the armed forces on sentry duty to inspect the MyKad.

104 Regulation 7(3).

105 'Police to Get 1557 Units to Read MyKad', *New Straits Times* (Malaysia), 28 February 2002, 4.

Apart from these categories of officers, it is an offence for any other person to unreasonably detain another's MyKad.[106] It is also an offence for any public officer to publish or communicate to any person the information contained in the register or any record made under the *NRA* or the Regulations, unless this is in the public interest *and* has the approval of the Director-General or is for the purpose of criminal proceedings.[107]

The personal information in the MyKad must be stored in duplicate in a register that is kept and maintained by the Director-General.[108] The register includes any microfilm, computer records, or any other means of storage of the particulars required to be maintained on the register.[109]

Regulation 12(1) of the Regulations stipulates that the register is not open to public inspection. Rather, it can only be inspected by duly authorised officers. Nevertheless, an extract of the register may, at the discretion of the Director-General, be issued to such authorised officers or to any member of the public upon payment of a fee.[110] Furthermore, the Director-General has discretion to publish information derived from the register.[111]

Except as highlighted above, the *NRA* — although it is the primary legislation governing the MyKad — does not provide for control over the collection of personal information and the purpose for which that information may be used by 'authorised' users. Neither does the *NRA* provide for the different levels of access rights or control measures over the central register (or database) that should be implemented to ensure the integrity of the MyKad system. The *NRA*, *RTA* and the Regulations confer only limited protection against the unauthorised use or disclosure of the personal information stored in the MyKad. Various other statutes protect certain aspects of the personal information in the MyKad, such as health information[112] and financial information,[113] but also to only a limited extent.

106 Regulation 8A. The word 'unreasonably' is not defined in the Regulations.

107 Regulation 25(1)(k). This offence is punishable by a term of imprisonment of not more than three years and/or a fine not exceeding RM20 000.

108 *NRA* s 4; reg 11. The duplicate includes the image or memory of the MyKad that is stored electronically: reg 11(2).

109 Regulation 11(1).

110 Regulation 12(2).

111 Regulation 20.

112 The health information required to be incorporated in the MyKad pursuant to sch 1A to the Regulations has a very wide scope and deals with sensitive material. There does not seem to be any specific statutory protection against disclosure of this information, except in so far as provided indirectly by the *Private Healthcare Facilities and Services Act 1998* (M'sia), which is limited in application to private healthcare facilities: see s 112(1), which empowers the Director-General of the Ministry of Health to direct a private healthcare facility to provide information relating to the condition, treatment or diagnosis of any of its patients. See also s 112(4), which limits this directive, requiring the Director-General to obtain the prior consent of the patient or his or her representative. There are no equivalent provisions applicable to public or government funded healthcare facilities.

113 Financial information in the MyKad is regulated by the information and secrecy provisions of the *Banking and Financial Institutions Act 1989* (M'sia). Sections 96, 97 and 98 prohibit the unauthorised disclosure of financial information which is identifiable to a particular individual. Section 99, however, permits the disclosure of financial information where such disclosure is authorised by any other written law for the purpose of investigating offences or in aid of any criminal or civil proceedings. It is uncertain whether there is sufficient protection against the possibility of

Several other statutes also indirectly protect the personal information stored in the MyKad and the corresponding databases. To begin with, the *Computer Crimes Act 1997* (M'sia) ('*CCA*') provides for offences relating to the misuse of computers. Any person who, without authorisation, uses a computer to access any program or data held in any computer or computer network, commits an offence.[114] Similarly, an offence is committed if unauthorised access is obtained with the intent to commit or facilitate a further offence of fraud or dishonesty under the *Penal Code*.[115] Access to any program or data is unauthorised where the individual is not personally 'entitled to control access of the kind in question' and does not have consent or exceeds any right or consent to such access given by a person so entitled.[116] These offences are punishable by a term of imprisonment ranging from three to 10 years, or a fine ranging between RM25 000 and RM100 000, or both.[117] Thus, the *CCA* provides some degree of protection against the unauthorised use or disclosure of personal information contained in the MyKad system.[118]

Under the *Communications and Multimedia Act 1998* (M'sia), any person who without lawful authority intercepts any communications or discloses such intercepted communications by means of any network facilities or network service commits an offence punishable by a term of imprisonment not exceeding one year, or a fine not exceeding RM50 000, or both.[119]

Any public official who, having in his or her possession an official secret,[120] 'fails to take reasonable care of, or so conducts himself as to endanger the safety or secrecy of [the] official secret,' commits an offence under the *Official Secrets Act 1972* (M'sia).[121] Thus the protection that the Act may confer in respect of information held in the MyKad databases is limited to information classified as an 'official secret' within the scope of that Act.

unauthorised use of the MyKad where a bank or financial institution lawfully retains a MyKad that has been swallowed in the process of an ATM transaction. Section 119, which regulates electronic fund transfers, does not provide for this type of situation.

114 *CCA* s 3. The *CCA* is one of the laws enacted by the Malaysian government as part of its MSC project.

115 *CCA* s 4.

116 *CCA* s 2(5).

117 *CCA* s 5.

118 See generally *CCA* s 5. The Act also supplements some of the existing provisions in the *Penal Code*, which provides for the offences of fraud (ss 206–10), dishonesty (ss 403–4), theft (s 378) and criminal breach of trust (ss 405, 407–9) in the event that there is unauthorised use or disclosure of, or even tampering with, the personal information contained in the MyKad through the misuse of computers or computer networks.

119 Sections 233–4. This Act is another of the laws enacted by the government as part of its MSC project.

120 Section 2 of the *Official Secrets Act 1972* (M'sia) defines an official secret as including documents and any corresponding information which relate to national security or which may be classified as 'secret' or 'confidential' by the relevant Minister or public officer.

121 Section 8(1)(iv). An offence under this section shall be punishable by between one and seven years of imprisonment.

B *Common Law Position*

Malaysia inherited the English common law and rules of equity as they existed in 1956,[122] and the Malaysian courts have since closely followed the development of the common law in England and other Commonwealth jurisdictions such as Australia. No common law right to general privacy or, in particular, information privacy has been recognised by Malaysian courts. While the superior courts of England[123] and of Australia[124] have considered and rejected an explicit recognition of a common law tort of invasion of privacy, this issue has yet to be considered by the Malaysian appellate courts.[125]

At present, the protection of personal information in Malaysia against misuse or unauthorised disclosure is merely incidental to the protection of other interests recognised by the common law under particular torts. In relation to information privacy, these torts include, but are not limited to, breach of confidence, defamation or the tort of malicious falsehood, and negligence.

An action for breach of confidence can only arise if three elements are satisfied: the personal information disclosed must have 'the necessary quality of confidence about it',[126] the information must have been imparted in circumstances importing an obligation of confidence and there must have been an unauthorised use or disclosure of the information by the party who was under

122 *Civil Law Act 1956* (M'sia) s 3. This is provided that there is no inconsistency between the common law or rules of equity of England and any written law in Malaysia, and is subject to qualifications required for local circumstances.

123 See, eg, *Kaye v Robertson* (1991) 18 FSR 62. In *Douglas v Hello! Ltd* [2001] 2 WLR 992, the English Court of Appeal, when considering an action for breach of confidence, was willing to concede that the law in England subsequent to the enactment of the *Human Rights Act 1998* (UK) c 42 (arising from art 8 of the European *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) ('*ECHR*')) recognises and will appropriately protect a right of personal privacy. In the recent decision of the House of Lords in *Wainwright v Home Office* [2003] 4 All ER 969, Lord Hoffmann (with whom the other Law Lords agreed) rejected the recognition of a common law tort of invasion of privacy, and held that ss 6 and 7 of the *Human Rights Act 1998* (UK) c 42 provided for statutory remedies in the event that there was a breach of privacy of any person pursuant to art 8 of the *ECHR*.

124 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 ('*Victoria Park Racing*'); see also Patrick Quirk and Jay Forder, *Electronic Commerce and the Law* (2nd ed, 2003) 335. However, the High Court of Australia in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 ('*Lenah*'), although not directly considering the question, opened the possibility of future recognition of a common law tort of invasion of privacy. The judgments of Gummow and Hayne JJ (at 248–50) and Callinan J (at 320–30) appeared not to regard the decision in *Victoria Park Racing* (1937) 58 CLR 479 as an insurmountable obstacle to the recognition of such a tort in Australia: see William Heath, 'Possum Processing, Picture Pilfering, Publication and Privacy: *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*' (2002) 28 *Monash University Law Review* 162, 175–7. In *Grosse v Purvis* [2003] QDC 151, a Queensland District Court judge, referring to comments in *Lenah* (at [422]–[438]), held that there was an actionable right to privacy (at [442]); see also Robert Dean, 'A Right to Privacy?' (2004) 78 *Australian Law Journal* 114, 114.

125 In a recent Malaysian High Court decision, the judge relied on *Kaye v Robertson* (1991) 18 FSR 62 in holding that there was no common law actionable right to privacy in Malaysia because this right was not recognised by the English common law: *Ultra Dimension Sdn Bhd v Kook Wei Kuan* [2004] CLJ 285, 289.

126 *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203, 215 (Lord Greene MR).

such obligation.[127] In England and Australia, a number of cases have confirmed that a cause of action for breach of confidence will arise to protect personal information imparted to a third party who has knowledge or ought to have knowledge of the confidentiality of such information.[128] These cases confirm that such an action protects not only information provided *by* the individual, but also information *about* that individual.[129]

In Malaysia, the action for breach of confidence has been raised in limited circumstances, namely in respect of trade secrets imparted for commercial reasons[130] or in the context of disclosure under legal compulsion.[131] There have been no Malaysian cases which have explored the extent of protection conferred under an action for breach of confidence for the unwarranted disclosure of personal information obtained in circumstances of confidence. It is nevertheless arguable that such an action can be used to protect individuals in the event that the information given by them or about them (and stored in the MyKad) is disclosed by public officials or the government, since this information is clearly imparted in confidence. However, such an action may not be successful if the disclosure of the personal information is made in the public interest.[132]

An action for defamation or for malicious falsehood can only be brought if there is disclosure of inaccurate or false personal information. These torts cannot be used to protect against the misuse of accurate personal information.[133] Hence, the actions can only be sustained in limited circumstances — when there is a disclosure of incorrect or false personal information that may be stored in the MyKad.

It is also possible for personal information to be protected against unauthorised or even authorised disclosure through the tort of negligence in situations where there has been negligent disclosure by the government or by public officials. A duty of care can arguably be imputed to the collection, processing and use of personal information by the government and its agencies with respect to the MyKad.[134] Any breach of this duty that results in foreseeable damage can give rise to a remedy available to the MyKad holder.

Injunctive relief would be available to the MyKad holder who successfully establishes a cause of action for breach of confidence or negligence. Whilst damages may provide a remedy for breach of confidence or negligence, the damages awarded would be limited only to mental distress or injury to feelings.[135] In most instances, the damage suffered due to the disclosure of personal

127 Ibid; *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41.
128 *X v Y* [1988] 2 All ER 648; *G v Day* [1982] 1 NSWLR 24.
129 John Fleming, *The Law of Torts* (9th ed, 1998) 672.
130 *Schmidt Scientific Sdn Bhd v Ong Han Suan* [1997] 5 MLJ 632.
131 *A-G (Hong Kong) v Zauyah Wan Chik* [1995] 2 MLJ 620.
132 Wacks, *Personal Information*, above n 65, 53–4; Allison Coleman, 'Protecting Confidential Information' in Chris Reed and John Angel (eds), *Computer Law* (5th ed, 2003) 259, 267–70.
133 Fleming, above n 129, 671.
134 Heliliah Yusof, 'Legal Issues in the Implementation of a Multipurpose Card' (Paper presented at the MSC International Cyberlaws Conference, Kuala Lumpur, 26 May 2000) 24.
135 Gerald Dworkin, 'The Common Law Protection of Privacy' (1967) 2 *University of Tasmania Law Review* 418, 442–3.

information lies in the disclosure itself being an infringement of information privacy, for which damages are an inadequate remedy.

C *Some Observations*

Although there is some statutory protection of personal information stored in the MyKad and the corresponding databases against unauthorised disclosure and misuse, the statutes examined above have several shortcomings. They provide only incidental protection against unauthorised use or disclosure of the MyKad holder's personal information. They give an individual very limited access to his or her personal information and no right to check for inaccuracies or make corrections. The statutes also only provide for criminal sanctions against the offenders, without conferring any right to civil remedies upon the victim. More significantly, they do not protect against the 'authorised' use and disclosure of personal information.

The existing statutory framework in Malaysia does not directly protect information privacy, but rather confers limited protection on a piecemeal basis. This is not surprising, since the existing statutes have been developed to pursue different policies and are enforced by diverse agencies.

The common law position in Malaysia on the protection of information privacy is erratic at best and does not confer adequate protection against the disclosure and misuse of personal information contained in the MyKad. Unless a particular set of facts falls within an established head of tort liability, the MyKad holder will not have a right of redress under the common law. In addition, the *Public Authorities Protection Act 1948* (M'sia) imposes a limitation of three years for the commencement of any civil action against the government concerning an act of default or neglect performed in the execution of duties under any written law.[136]

The deficiencies inherent in the existing statutory framework and the hurdles within the common law discussed above expose an urgent need for a comprehensive legal framework to address the information privacy concerns arising from the implementation of the MyKad project. Whether or not the recent draft Personal Data Protection Bill 1998 (M'sia) ('PDP Bill') proposed by the government addresses these concerns will now be considered.[137]

[136] Section 2(a). The normal period of limitation for any tort action is six years: *Limitation Act 1953* (M'sia) s 6(1).

[137] The only draft that has been issued by the Ministry of Energy, Communications and Multimedia is the PDP Bill dated 21 February 2000. Since then, there have been several announcements by the government and the Ministry of Energy, Communications and Multimedia that the final draft of the PDP Bill would soon be enacted as law: Raslan Sharif, 'Data Protection Law to Balance Private, Public Interests', *The Star* (Malaysia), 4 December 2001, In Tech 3; Syed Azhar, 'New Law to Punish Firms Which Leak Data on Clients', *The Star* (Malaysia), 5 November 2002, 8; Kar Yean Lee, 'Govt Ready to Enact Privacy and Data Protection Law', *The Star Online* (Malaysia), 24 January 2003 <http://thestar.com.my/services.printerfriendly.asp?file=/2003/1/24/business>; and, more recently, Jin Hun Chong, 'New Cyber Law to Strengthen Protection of Personal Data', *Business Times* (Malaysia), 14 May 2004, 2. However, as at July 2004, no further draft of the PDP Bill has been made available to the public or tabled in Parliament.

V THE PERSONAL DATA PROTECTION BILL

A *Background to the Personal Data Protection Bill*

The protection of information privacy has not been a feature of the Malaysian government's traditional culture or political agenda over the years. The government has had access to the comprehensive personal information of Malaysians pursuant to various statutes[138] and is the biggest 'user' of such personal information in Malaysia.[139]

However, in line with Malaysia's commitment to the MSC, the draft PDP Bill was formulated and released for public consideration in 2000.[140] The objectives of the PDP Bill are to provide adequate security and privacy for the handling of personal information, to encourage confidence among consumers and users of industries and to accelerate the usage of electronic transactions.[141] The rationale for the PDP Bill is to promote Malaysia as a world-class hub of communications and multimedia and a premier base for foreign high technology investments.[142] Hence, the primary driver of this shift in policy in favour of the protection of personal information is the economic necessity of greater confidence in the electronic marketplace, rather than a realisation of the inherent importance of information privacy.[143]

Although the PDP Bill is modelled on Hong Kong's *Personal Data (Privacy) Ordinance 1997* ('the Hong Kong Ordinance'), the PDP Bill in its current draft form has a uniquely Malaysian flavour which may restrict the ambit of the protection, particularly in respect of information stored in the MyKad.

The next part of this article will examine some of the more obvious limitations inherent in the PDP Bill which will have an adverse impact on the protection of personal information relating to the MyKad.

B *Scope of Protection*

At first glance the PDP Bill seems to have wide coverage, since it is applicable to both the private and public sectors. It binds the government and treats each government department as having a separate identity.[144] Section 4(1) of the PDP Bill requires that all collection, holding, processing or use of personal data by any data user must comply with all of the nine Data Protection Principles

138 See, eg, regs 7(1), 12(1) read together with *NRA* s 6; *RTA* s 58(2); *Official Secrets Act 1972* (M'sia) s 11; *Internal Security Act 1960* (M'sia) ss 8, 65, 73.

139 Yusof, above n 134, 4–5, 28.

140 Public consideration of the PDP Bill has not been on a large scale — selected public and private sector groups were formally requested to give their feedback and comments: Sharif, above n 137. However, this consultation was in respect of the 21 February 2000 version of the PDP Bill. To this author's knowledge, there has not been any open public consultation on subsequent drafts.

141 Ministry of Energy, Communications and Multimedia, Malaysia, *Personal Data Protection* <http://www.ktkm.gov.my>.

142 Ibid.

143 The government has already announced its position that the PDP Bill attempts to balance an individual's information privacy rights with competing public and private interests: Sharif, above n 137.

144 PDP Bill s 3.

('DPPs')[145] unless the PDP Bill provides otherwise. The DPPs confer protection in respect of various aspects of the personal data falling within the ambit of the PDP Bill, including the manner and purpose of its collection as well as its use and disclosure, accuracy, time of retention, accessibility, correction and security.

The definition of 'personal data' in the PDP Bill is sufficiently wide to encompass the personal information recorded in the MyKad and in the corresponding databases.[146] However, the PDP Bill defines a 'data user' as

> a person who either alone or jointly with other persons, controls the collection, holding, processing or use of the personal data *but does not include any person who collects, holds, processes or uses* [that data] *solely on behalf of another person*.[147]

This exception is not contained in the definition of 'data user' under the Hong Kong Ordinance.[148] This definition in the PDP Bill will give rise to a difficulty in identifying the data user or users — especially where one government department receives services from another.[149] The fact that the NRD may employ other government departments[150] to assist with the collection, holding, processing or use of the personal information in the MyKad could arguably mean that these other government departments are not data users and are therefore excluded from regulation by the PDP Bill. This exception would apply even if these government departments process or use the personal information when assisting the NRD.

The officers or employees of these government departments or, for that matter, the NRD, would also be excluded from the scope of regulation by the PDP Bill since they would be acting on behalf of their employer. There is no provision in the PDP Bill to impose vicarious liability on the government, as an employer, for

145 These are set out in sch 1 to the PDP Bill and are: (1) 'Manner of collection of personal data'; (2) 'Purpose of collection of personal data'; (3) 'Use of personal data'; (4) 'Disclosure of personal data'; (5) 'Accuracy of personal data'; (6) 'Duration of retention of personal data'; (7) 'Access to and correction of personal data'; (8) 'Security of personal data'; and (9) 'Information to be generally available'.

146 'Personal data' is defined in s 2(1) of the PDP Bill as meaning

> any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user, including any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual.

147 Section 2(1) (emphasis added). The word 'person' is defined in the *Interpretation Acts 1948 and 1967* (M'sia) as including 'a body of persons, corporate or incorporate'. This definition would therefore include firms, companies, associations, government departments, authorities and organisations.

148 Section 2(1). But see s 2(12) of the Hong Kong Ordinance which states that:

> A person is not a data user in relation to any personal data which the person holds, uses or processes solely on behalf of another person if, but only if, that first mentioned person does not hold, process or use as the case may be, those data for any of his own purposes.

See also Paul Stephenson, Alisa Kwan and David Ellis, *Cyberlaw in Hong Kong* (2001) 223.

149 Abu Bakar Munir and Siti Hajar Mohd Yasin, *Privacy and Data Protection*: *A Comparative Analysis with Special Reference to the Malaysian Proposed Law* (2002) 184.

150 These include, among many, the Road Transport Department, the Immigration Department and the Royal Malaysian Police.

wrongful acts committed by employees in the course of their employment.[151] What happens, then, if these government departments or their officers or employees act in an unauthorised manner in using or disclosing the personal information in the MyKad?

The consequence of the above limitation on the scope of protection provided by the PDP Bill is that the avenues of redress for a MyKad holder are severely restricted. A MyKad holder whose information privacy has been infringed through unauthorised means by persons other than the data user would have no right to lodge a complaint[152] or to seek compensation for damage or distress,[153] since both these avenues are available only when the contravention is committed by a data user. Notwithstanding the criminal sanctions provided under the PDP Bill,[154] a MyKad holder has no civil remedy against government departments or officers who process, use or disclose the cardholder's personal information in an unauthorised manner.

One way to address the above limitation would be to remove the exception in the definition of 'data user' or, alternatively, to restrict the application of that exception to situations where a person does not hold, process or use the personal data for his or her own purposes, regardless of whether these purposes are authorised or unauthorised.

Another limitation is that in the event of an inconsistency between the PDP Bill and any other written law — for example, the *NRA* or the *RTA* — the provisions of that written law shall prevail to the extent of that inconsistency[155] unless the written law is listed in sch 5 to the PDP Bill.[156] Effectively this means that there is a possibility that the PDP Bill would not even apply to the *NRA* in terms of the collection, use and disclosure of personal information as provided for in that statute. Since the *NRA* is the primary legislation regulating the collection and use of personal information in Malaysia, it must be subject to the fundamental principles of data protection as established by the DPPs in the PDP Bill. This could be easily achieved by the inclusion of the *NRA* in sch 5 to the PDP Bill.

C *Data Matching*

As mentioned above,[157] one of the main privacy implications of the MyKad is the potential for extensive data surveillance by the government or its enforcement agencies. Personal information records held in different databases can be linked by using a cardholder's unique PIN. This poses a serious privacy risk to the MyKad holder, who may be unaware that he or she is the subject of such

151 This is unlike the position in Hong Kong where s 65 of the Hong Kong Ordinance specifically provides for such liability of employers and principals.
152 PDP Bill s 57(1).
153 PDP Bill s 88.
154 Section 89.
155 PDP Bill s 108(1).
156 PDP Bill s 108(2). At present, there is no written law specified in sch 5 to the PDP Bill.
157 See above Part III(B)(1).

scrutiny, whose data is used for a purpose other than that for which it was collected, and who may consequently be subject to an adverse action being taken against her or him. Data matching by government organisations 'is often likened to a "fishing expedition"',[158] involving the mass surveillance of individuals, without prior indication of violations or cause for suspicion, in order to identify 'suspect' individuals (whether correctly or incorrectly) through 'hits' from the data matching process.[159]

The PDP Bill imposes some restrictions on data matching.[160] DPP 3 provides that personal data 'shall not, without the consent of the data subject, be used for any purpose other than [that] for which the personal data were to be used at the time of … collection'[161] or for a directly related purpose. In addition, s 48 of the PDP Bill provides that data matching is prohibited unless it has the consent of the subject in question and either the Commissioner for Personal Data Protection[162] has also consented or the procedure falls within a class approved by the Minister. Specific procedures set out in that section must be complied with in order to secure such consent. An additional protection conferred by this section is that a data subject may challenge the results of data matching within seven days of receiving a written notice that specifies and offers reasons for the adverse action the government proposes to take.[163]

However, the protections in s 48 of the PDP Bill are subject to a severe limitation. Section 51 of the PDP Bill expressly excludes the application of s 48 'to a government department, statutory body or local authority proposing to carry out a matching procedure' where written notice of such matching procedure has been given to the Commissioner. This means that any government department, including the NRD and any other enforcement agency, can carry out matching procedures with impunity once written notice has been given to the Commissioner. Arguably, these government departments, if falling within the definition of 'data user' and if not exempted from the application of the PDP Bill,[164] would contravene DPP 3 since the purpose for carrying out data matching in itself constitutes a purpose different from that for which the data was originally collected. However, the exception in s 51 of the PDP Bill considerably weakens the protection conferred by that Bill against data matching and therefore

158 Munir and Yasin, above n 149, 101.

159 See ibid 106.

160 A 'matching procedure' is defined in s 2(1) of the PDP Bill as involving an automatic comparison of personal data (collected for a purpose or purposes in respect of at least 10 data subjects), where that comparison is for verifying data that 'may be used for the purpose of taking adverse action against any of the data subjects' or where it may be reasonably believed that the data could practicably be used in this way.

161 PDP Bill sch 1, Principle 3(1).

162 The Commissioner is appointed under s 5(1) of the PDP Bill.

163 Section 2(1) of the PDP Bill defines 'adverse action' to mean 'any action that may adversely affect an individual's rights, benefits, privileges, obligations or interests'. Notably, s 2(1) of the Hong Kong Ordinance also includes 'legitimate expectations' in its definition of 'adverse action', though it does not define this term. The phrase 'legitimate expectations' was first used in *Schmidt v Secretary of State for Home Affairs* [1969] 2 Ch 149 to indicate that an expectation or interest that is short of a legal right may nevertheless warrant the protection of the rules of natural justice: at 170 (Lord Denning MR).

164 See below Part V(D).

increases the risk of intrusion into individuals' private information by the government.

The only way to address this limitation in the PDP Bill is to remove s 51 altogether. It is interesting to note that there is no corresponding provision in the Hong Kong Ordinance.

D *Exemptions*

Like other personal data legislation, the PDP Bill, in Part X, contains a number of exemptions.[165] These reflect the Malaysian government's reluctance to relinquish control over its citizens:

> [The PDP Bill] proposes several exemptions to meet the unique nature and requirements of certain activities and bodies. … Some government agencies and departments feel that their work might be hampered if no exemptions were given. … Legitimate national security needs could be the subject of an exemption.[166]

Moreover, the extent of these exemptions is wider than that provided for in other jurisdictions. For example, the Hong Kong Ordinance provides for an exemption from the principles of *use* and *access* only in the case of data held by or on behalf of the government for the purposes of safeguarding national security, defence or international relations.[167]

In Malaysia, however, the PDP Bill exempts data held for these purposes from the principles of collection, purpose, use, disclosure, access and correction.[168] The PDP Bill also confers on the relevant Minister the power to issue a certificate that will be treated as conclusive evidence that the exemption 'was required for the purpose of safeguarding national security, defence or international relations'.[169] On the basis of this certificate, the Commissioner may be directed not to inspect or investigate a particular complaint of non-compliance with the DPPs and the Commissioner is required by law to comply with this directive.[170] The certificate must identify the personal data to which it applies through a general description only and may have prospective effect.[171]

165 Sections 72–87.

166 Sharif, above n 137, quoting Leo Moggie, the then Minister of Energy, Communications and Multimedia.

167 Section 57. The principle of *use* requires that personal data not be used, unless with the consent of the data subject, for purposes other than that for which the data was to be used at the time of collection or for directly related purposes: Hong Kong Ordinance sch 1, Principle 3. The principle of *access* requires that the data subject is entitled to ascertain whether a user holds the data subject's personal data, and has a right to request access to that personal data within a reasonable time: Hong Kong Ordinance sch 1, Principle 6.

168 Section 72. Section 72(1) exempts these types of data from Principles 1–4, 7 and 9.

169 Section 72(3). The corresponding provision in s 57(3) of the Hong Kong Ordinance does not contain the word 'conclusive'.

170 Section 72(6) of the PDP Bill.

171 Section 72(5) of the PDP Bill. It is uncertain what is meant by 'prospective effect' in this provision. The phrase suggests that the certificate may be issued to have future effect in respect of data yet to be collected, whereas the exemption in s 72(1) is in respect of data already 'held by or on behalf of the Government'. There is no corresponding provision in the Hong Kong Ordinance.

National security is not defined in the PDP Bill. The above provision therefore gives the Minister wide discretionary power to exempt personal information, held by or on behalf of the government in respect of the MyKad, from the main DPPs on the basis of safeguarding national security, simply by issuing a certificate to this effect. The certificate does not need to specify the exact reasons relied on by the Minister. In any case, the personal information on the MyKad could be considered to be a 'legitimate' national security issue since it relates to the identification of Malaysian citizens. Thus, this provision confers upon the Minister an excessive power because almost anything related to the MyKad could appear to give rise to a national security issue.

A more significant aspect of Part X of the PDP Bill is the wide and general power of exemption conferred on the relevant Minister,[172] who 'may, upon the recommendation of the Commissioner, exempt any personal data or class of personal data or any person or class of persons' from the DPPs and other provisions of the PDP Bill. The power is vested in the Minister '[n]otwithstanding other provisions of the [PDP Bill]'[173] and allows the Minister to 'impose any terms and conditions as he thinks fit' on the exemptions introduced.[174] This effectively gives the Minister a broad discretion to override the other provisions of the PDP Bill. There is no corresponding provision in the Hong Kong Ordinance. There is a grave danger that arbitrary use of this provision in the future could jeopardise the protection of certain types of personal information, including that stored in the MyKad.

This author contends that the exemption provisions in the PDP Bill should be restricted and should contain checks and balances to ensure that the Minister's power of exemption is not exercised arbitrarily. There must be restrictions in the PDP Bill to ensure that exemptions are permitted only in limited circumstances. Without such restrictions, it is very likely that the information in the MyKad will be exempt from the protection of the PDP Bill, either on the basis of national security or under the general power of exemption.

E *Independence of the Commissioner*

One of the cornerstones of any personal data protection legislation is the independence of the entity which is entrusted with the task of implementing and monitoring compliance with such legislation. An independent Commissioner is probably the most important precondition for a workable and efficient data protection framework.[175] An essential requirement is that there must be a clear separation between the Commissioner and those who are subject to the Commissioner's powers under the data protection framework. This degree of independence is lacking in the PDP Bill since the Commissioner is appointed by, and

172 Section 87(1).
173 Section 87(1).
174 Section 87(2).
175 Munir and Yasin, above n 149, 156, citing Spiros Simitis, a former Data Protection Commissioner of Hesse, Germany.

answerable to, the Minister with responsibility for personal data protection.[176] In rejecting the option of making the Commissioner answerable directly to Parliament under the PDP Bill, the Minister in question stated that 'our country is not yet at the stage where the Government can be left out of the loop.'[177]

This lack of independence will allow for potential accusations of bias or unfairness because the Commissioner's rulings will be subject to the overriding authority of the Minister and therefore the executive, especially if the Commissioner's rulings regarding the data are in favour of the government or its agencies. Such a lack of independence also casts doubt on the efficacy of the PDP Bill as a mechanism for protecting personal information from misuse, particularly government misuse.[178]

This inherent limitation in the PDP Bill destroys one of the Bill's objectives — the protection of information privacy — which in turn jeopardises its other objectives and its credibility. The PDP Bill will provide no real protection for personal information in Malaysia unless the Commissioner for Personal Data Protection is independent of the government. Simply ensuring that the Commissioner is appointed by and reports directly to Parliament, thereby taking this power out of the hands of the executive, could address this limitation.

F *A Case for Reform*

The PDP Bill, once enacted, will provide a statutory framework which confers a degree of protection of personal information that has previously not existed in Malaysia. The Bill will also confer certain rights on individuals whose personal information falls within its ambit. However, the limitations highlighted above demonstrate that some aspects of the PDP Bill may dilute its full potential in relation to the protection of personal information in the MyKad. The measures proposed by this author to strengthen information privacy are not technically difficult, but require a fundamental change of attitude towards the protection of information privacy on the part of the government. If this change is not forthcoming, the PDP Bill in its current form will not comprehensively protect personal information, such as that stored in the MyKad, against misuse.

In addition, the enactment of strengthened personal data protection legislation should be supported by judicial recognition of a constitutional right to information privacy. This would provide a comprehensive and effective legal framework for the protection of personal information in Malaysia.

176 Section 5(1), (4).

177 Sharif, above n 137, quoting Leo Moggie, the then Minister of Energy, Communications and Multimedia who was at that time also the Minister in charge of personal data protection in Malaysia.

178 This is especially so because the government is the largest data user of all: see above n 139 and accompanying text.

VI A CONSTITUTIONAL RIGHT TO INFORMATION PRIVACY

A *Information Privacy as a Human Right*

Article 12 of the *Universal Declaration of Human Rights* ('*UDHR*')[179] remains the international benchmark for the recognition of privacy as a human right. It provides that:

> No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks on his honour or reputation. Everyone has a right to the protection of the law against such interferences or attacks.

This right is similarly recognised in numerous other international conventions, including art 17 of the *International Covenant on Civil and Political Rights*.[180] Although Malaysia has yet to ratify this convention, it has been party to several declarations including the *Vienna Declaration and Programme of Action*[181] as well as the *Final Declaration of the Regional Meeting for Asia of the World Conference on Human Rights* ('*Bangkok Declaration*').[182] In both cases, Malaysia reaffirmed the universal nature of the rights and freedoms contained in the *UDHR*.[183]

This author contends that the right to information privacy is a basic, internationally recognised human right and is also protected by the fundamental guarantees enshrined in the *Malaysian Constitution*.

B *The Malaysian Constitution and the Court of Appeal*

The *Malaysian Constitution* is the supreme law in Malaysia. Article 5(1) of the *Malaysian Constitution* provides the fundamental guarantee that 'no person shall be deprived of his life or personal liberty, save in accordance with law.' In interpreting this provision, the Malaysian Court of Appeal, in what has been heralded as the high-water mark in constitutional law in Malaysia, has given a dynamic and liberal interpretation to the word 'life'.

In *Tan Tek Seng v Suruhanjaya Perkhidmatan Pendidikan*,[184] Sri Ram JCA, with whose judgment Fairuz J concurred, held that the word 'life' in art 5(1) did not refer to 'mere existence', but 'incorporates all those facets that are an integral part of life itself and those matters which go to form the *quality of life*'.[185] These facets include the right to livelihood and the right to live in a

179 GA Res 217A, UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/Res/217A (1948).

180 Opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

181 *Vienna Declaration and Programme of Action*: *Report of the World Conference on Human Rights*, UN Doc A/CONF.157/23 (1993).

182 UN Doc A/CONF.157/ASRM/8, A/CONF.157/PC/59 (1993).

183 See Sivarasa Rasiah, 'Making Law a Reality: Human Rights and Access to Justice' (Paper presented at the Bar Council's 50th Anniversary Commemorative Conference, Kuala Lumpur, 1997) 6.

184 [1996] 1 MLJ 261 ('*Tan Tek Seng*').

185 Ibid 288 (Sri Ram JCA) (emphasis added). In this case, the Court of Appeal held that a person had the right to seek and be engaged in lawful employment, the removal from which had to be in accordance with fair procedure.

reasonably healthy environment.[186] The right to livelihood and the right to work were held to be guaranteed under the *Malaysian Constitution*.[187] Sri Ram JCA further held that judges 'should, when discharging their duties as interpreters of the supreme law, adopt a liberal approach in order to implement the true intention of the framers of the [*Malaysian*] *Constitution*'.[188] In taking this approach, the Court of Appeal jettisoned the narrow and literal approach previously taken by the Malaysian courts in the interpretation and application of the *Malaysian Constitution*.[189]

A similar approach to art 5(1) of the *Malaysian Constitution* was taken in *Hong Leong Equipment Sdn Bhd v Liew Fook Chuan*.[190] Sri Ram JCA stated that the 'high standards of social justice' established within the *Malaysian Constitution* should not be deliberately lowered by the courts.[191] In *Sugumar Balakrishnan v Pengarah Imigresen Negeri Sabah*,[192] the expression 'personal liberty' in art 5(1) of the *Malaysian Constitution* was similarly construed in a broad and liberal fashion by the three judges of the Court of Appeal to include the liberty of an aggrieved person to seek redress from the courts, including judicial review. This was held to be one of the many facets of personal liberty guaranteed by this provision of the *Malaysian Constitution*.[193]

These cases are a reflection of the Court of Appeal's recent activism in translating the basic human rights protected by the *Malaysian Constitution* into 'real' rights applicable to all aspects of daily life. This gives national significance to rights previously not genuinely recognised or protected. The Court of Appeal has taken the view that a liberal reading of the *Malaysian Constitution* is necessary to give effect to its spirit and intention as a living and dynamic documentation of the supreme law of Malaysia.[194]

In arriving at the decisions in the cases above, the Court of Appeal has given constitutional recognition to derived rights or non-enumerated rights which flow from the express rights guaranteed by the *Malaysian Constitution*. In doing so, the Court of Appeal has relied on the spirit and intended meaning of art 8(1) of

186 Ibid.
187 Ibid.
188 Ibid.
189 This narrow and literal approach is evident in: *Karam Singh v Menteri Hal Ehwal Dalam Negeri* [1969] 2 MLJ 129; *Andrew Thamboosamy v Superintendant of Pudu Prisons* [1976] 2 MLJ 156; *Public Prosecutor v Khong Teng Khen* [1976] 2 MLJ 166; *Loh Kooi Choon v Malaysia* [1977] 2 MLJ 187; *Malaysia v Loh Wai Kong* [1979] 2 MLJ 33.
190 [1996] 1 MLJ 481 ('*Hong Leong Equipment*').
191 Ibid 510.
192 [1998] 3 MLJ 289 ('*Sugumar Balakrishnan*').
193 Ibid 308 (Sri Ram JCA). However, on appeal, the Federal Court (the highest court in Malaysia) held that the statute in question evidenced Parliament's express intention to exclude judicial review by the courts except on procedural grounds: *Pihak Berkuasa Negeri Sabah v Sugumar Balakrishnan* [2002] 3 MLJ 72, 93 (Dzaiddin FCJ). The Federal Court seemed to favour the contention of the appellant that 'personal liberty' in art 5(1) of the *Malaysian Constitution* referred to rights relating to the person or body of the individual as opposed to the liberty to seek judicial review in all cases.
194 See M P Jain, *Administrative Law of Malaysia and Singapore* (3rd ed, 1997) viii; Cyrus Das, '"Life" under Article 5: What Should It Be?' (2002) 31(4) *Insaf*: *The Journal of the Malaysian Bar* 68, 71.

the *Malaysian Constitution*, which provides that 'all persons are equal before the law and entitled to the equal protection of the law'.[195] By interpreting the express rights guaranteed in the *Malaysian Constitution* as being subject to the 'brooding omnipresence'[196] of art 8(1), the Court of Appeal has been able to give recognition to several derived rights. The Court of Appeal has effectively put into place a constitutional framework for the recognition and protection of basic human rights in Malaysian jurisprudence.

In these cases, the Court of Appeal also departed from the tradition of referring to common law developments in constitutional interpretation in England. It did so on the basis that the *Malaysian Constitution* is a written constitution without parallel in England.[197] Instead, the Court of Appeal looked at the wealth of jurisprudence from other Commonwealth nations with written constitutions similar to Malaysia's, particularly India, for the purpose of giving recognition to these derived rights.[198] While the Court of Appeal has yet to recognise the right to information privacy or the right to privacy as derived from the right to 'life' and to 'personal liberty', the Indian Supreme Court has already recognised a right of privacy under the *Indian Constitution*.

C *The Indian Experience*

In *Kharak Singh v Uttar Pradesh*,[199] a majority in the Indian Supreme Court held that 'personal liberty'[200] is a 'compendious term to include within itself all the varieties of rights which go to make up the "personal liberties" of man'.[201] The majority, however, stopped short of recognising a right of privacy. In a strong dissenting opinion, Rao J was of the view that the words 'life' and 'personal liberty' in art 21 of the *Indian Constitution* were comprehensive enough to include a right to privacy:

> the right to personal liberty takes in not only a [person's] right to be free from restrictions placed on his movements, but also [a right to be] free from encroachments on his private life. It is true [that] our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an

195 See Gopal Sri Ram, 'The Role of Judges and Lawyers in Evolving a Human Rights Jurisprudence' (January 2003) *Infoline*: *The Official Newsletter of the Malaysian Bar* 17, 20.

196 *Maneka Gandhi v India*, AIR 1978 SC 597 (Bhagwati J) ('*Maneka Gandhi*'), approved by the Malaysian Court of Appeal in *Sugumar Balakrishnan* [1998] 3 MLJ 289, 305 (Sri Ram JCA).

197 One explanation given for the lack of recognition of a right to privacy has been the lack of a constitutional basis for doing so in England and Australia. While this lack of recognition is now addressed by the enactment of the *Human Rights Act 1998* (UK) c 42, the lack of broad, fundamental rights in the *Australian Constitution* may still pose some constraints on the recognition of a right to privacy as a fundamental right in Australia: see Greg Taylor, 'Why Is There No Common Law Right of Privacy?' (2000) 26 *Monash University Law Review* 235, 272–4.

198 *Tan Tek Seng* [1996] 1 MLJ 261, 281–9 (Sri Ram JCA); *Hong Leong Equipment* [1996] 1 MLJ 481, 542–3 (Sri Ram JCA); *Sugumar Balakrishnan* [1998] 3 MLJ 289, 305–8 (Sri Ram JCA); see also Das, above n 194, 72–3.

199 AIR 1963 SC 1295 ('*Kharak Singh*'). This case concerned a challenge brought by the petitioner to the constitutional validity of the Uttar Pradesh Police Regulations which authorised home visits and the surveillance of persons under suspicion by the police.

200 *Indian Constitution* art 21. See also art 5(1) of the *Malaysian Constitution*, which is similarly worded.

201 *Kharak Singh*, AIR 1963 SC 1295, 1302 (Ayyangar J).

> essential ingredient of personal liberty … We would, therefore, define the right of personal liberty in Art 21 as a right of an individual to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures.[202]

In *Govind v Madhya Pradesh*,[203] a later decision of the Indian Supreme Court, Mathew J approved the minority judgment of Rao J in *Kharak Singh*[204] and held that art 21 of the *Indian Constitution* conferred a right to privacy. In doing so, Mathew J observed that '[t]here can be no doubt that the makers of our *Constitution* wanted to ensure conditions favourable to the pursuit of happiness',[205] but stressed that the right to privacy would necessarily develop on a case-by-case basis.[206]

In *Maneka Gandhi v India*,[207] the Indian Supreme Court reaffirmed the wide interpretation of art 21 of the *Indian Constitution* taken thus far by that Court. It stated that the correct way to interpret constitutional provisions that conferred fundamental rights was 'to expand the reach and ambit of [those] rights rather than attenuate their meaning and content by a process of judicial construction'.[208] The expression 'personal liberty' therefore covered 'a variety of rights which go to constitute the personal liberty'[209] of a person. Further, the Indian Supreme Court held that art 21 should be read subject to the equality provision in art 14 of the *Indian Constitution*, which aims to minimise arbitrary state action and ensure fairness and equality of treatment.[210]

More recent Indian cases[211] have developed the protection of the right to privacy provided by art 21 read together with art 14 of the *Indian Constitution* by extending its protection to include unauthorised publication of a person's life story and the interception of telephone communications. While all of these Indian cases have recognised a general right of privacy, there is nothing to

202 Ibid 1306.

203 AIR 1975 SC 1378 ('*Govind*'). The circumstances and findings of this case were similar to those of *Kharak Singh*, AIR 1963 SC 1295.

204 *Kharak Singh*, AIR 1963 SC 1295, 1303 (Rao J). Mathew J also relied on the American cases of *Griswold v Connecticut*, 381 US 479 (1965) and *Roe v Wade*, 410 US 113 (1973) in arriving at his decision in this case: *Govind*, AIR 1975 SC 1378, 1383.

205 *Govind*, AIR 1975 SC 1378, 1384.

206 Ibid. Mathew J also observed that any right to privacy must 'encompass and protect the personal intimacies of the home, the family, marriage, motherhood, procreation and child rearing' but that this catalogue did not give a full picture of the distinctive characteristics of the right to privacy, since more subtle and far-reaching means of invading privacy arise over time: at 1385.

207 AIR 1978 SC 597. This landmark decision in constitutional law in India was relied upon heavily by the Malaysian Court of Appeal in giving a liberal interpretation to the *Malaysian Constitution* in *Sugumar Balakrishnan* [1998] 3 MLJ 289.

208 *Maneka Gandhi*, AIR 1978 SC 597, 622 (Bhagwati J).

209 Ibid.

210 Ibid 624. Therefore no person should be deprived of life or personal liberty, save in accordance with a procedure established by law, and that procedure must be right, just and fair and not arbitrary.

211 *R Rajagopal v Tamil Nadu*, AIR 1995 SC 264, 269–77; *People's Union for Civil Liberties v India*, AIR 1997 SC 1203. See also Pravin Anand and Gitanjli Duggal, 'India' in Michael Henry (ed), *International Privacy, Publicity and Personality Laws* (2001) 233, 241–2.

prevent refinement of this recognition along the same lines as the more specific right of information privacy.

D *A Constitutional Right*

Both the Malaysian and Indian cases referred to above lend support to this author's contention that the right to information privacy as a mechanism for the protection of personal information stored in the MyKad can and should be recognised as a fundamental right protected by the *Malaysian Constitution*.

In view of the liberal and dynamic manner in which the Malaysian Court of Appeal has construed 'life' and 'personal liberty' in art 5(1) read together with art 8(1) of the *Malaysian Constitution*,[212] it is arguable that a person's right to information privacy is inherent within the right to life and personal liberty under the *Malaysian Constitution*. This right is relevant to the 'quality of life' and 'personal liberty' of the individual citizen. Recognition of such a right by derivation from the *Malaysian Constitution* in a manner already embarked upon by the Malaysian Court of Appeal depends on continued judicial activism.[213]

If the right to information privacy is placed on a constitutional footing, individuals would have recourse to public law remedies[214] for the enforcement of fundamental rights conferred by the *Malaysian Constitution*. This would include the award of compensation to citizens whose fundamental rights have been infringed due to acts or omissions by the government. Private law remedies would also be available.[215]

A constitutional right to information privacy would not be absolute, but subject to any compelling and overriding national interest. However, the courts would be able to scrutinise the claim of overriding national interest and not simply accept the public decision-maker's mere *ipse dixit* on the question.[216]

A constitutional right to information privacy would both confer public law protection upon citizens and influence private law developments relating to the

[212] The decision of the Federal Court in *Pihak Berkuasa Negeri Sabah v Sugumar Balakrishnan* [2002] 3 MLJ 72 may unfortunately dilute the significant advances made thus far by the Court of Appeal in developing a vibrant constitutional jurisprudence recognising basic human rights in Malaysia. In coming to its decision, the Federal Court felt bound by an earlier Federal Court decision in *Malaysia v Loh Wai Kong* [1979] 2 MLJ 33: *Pihak Berkuasa Negeri Sabah v Sugumar Balakrishnan* [2002] 3 MLJ 72, 101 (Dzaiddin FCJ). However, it must be noted that the Federal Court decision in *Malaysia v Loh Wai Kong* [1979] 2 MLJ 33 was based on a literal approach to constitutional interpretation following an old Indian case (*Gopalan v Madras*, AIR 1950 SC 27) which preceded the constitutional high-water mark decision of the Indian Supreme Court in *Maneka Gandhi*, AIR 1978 SC 597: Das, above n 194, 76–7. Outside the Court of Appeal, the Malaysian judiciary has been hesitant and tentative in embracing a constitutional basis for human rights jurisprudence or in breaking out of the constraints currently restricting the versatility and dynamism inherent in the principles contained in arts 5(1) and 8(1) of the *Malaysian Constitution*: at 77–80. See the recent Federal Court decision in *Danaharta Urus Sdn Bhd v Kekatong Sdn Bhd* [2004] 2 MLJ 257 (Paul JCA) where the Federal Court applied art 8(1) of the *Malaysian Constitution* in a narrow manner.

[213] See generally Sri Ram, above n 195, 20.

[214] These would include relief provided for under para 1 of the schedule to the *Courts of Judicature Act 1964* (M'sia), namely, writs of habeas corpus, mandamus, prohibition and certiorari, as well as such other relief as may be moulded by the courts according to the justice of the case: ibid 22.

[215] *Maharaj v A-G (Trinidad and Tobago) [No 2]* [1979] AC 385.

[216] *Hong Leong Equipment* [1996] 1 MLJ 481, 537 (Sri Ram JCA).

misuse of personal information. The recognition of such a constitutional right would also provide a strong foundation for more rigorous personal data protection legislation in Malaysia.

VII CONCLUSION

There is no doubt that the MyKad has the main security features that a smart card should have given the present level of technological development.[217] However, a distinction must be made between security concerns and the information privacy implications of the MyKad. The information privacy implications highlighted in this article arise notwithstanding the use of technologically advanced security features. The real threat to information privacy arises as a result of the amount and types of personal information in the MyKad and due to the networking of databases within which such information is stored. This threat to information privacy can only be addressed by a robust legal framework which protects personal information against misuse, whether by the government or other parties.

The existing legal framework is lacking in this respect and confers little protection on MyKad holders. The current laws also fail to support or inculcate a basic respect for information privacy as a human right. All democratic societies must respect information privacy to protect the democratic ideal. Information privacy is one of the universal virtues of a democratic nation that transcends cultural value systems.

If the MyKad is meant to be a tool to better serve the citizens of Malaysia, then there is no excuse for the government to refuse to implement a robust and information privacy-focused personal data protection legislation. Such legislation requires as its foundation the recognition of information privacy as a basic human right, in order to ensure that personal information stored in the MyKad is protected against 'authorised' and unauthorised use or disclosure of such personal information. As demonstrated in this article, this foundation already exists within the *Malaysian Constitution* — it merely requires judicial recognition by the Malaysian courts. Once the protection of information privacy is placed on a constitutional footing and strong personal data protection legislation providing for an independent Commissioner is enacted, there will be impetus for the development of a culture of respect for information privacy within the government, its bureaucracy and the people of Malaysia.[218]

[217] Smart Card Alliance, *Privacy and Secure Identification Systems*: *The Role of Smart Cards as a Privacy-Enabling Technology* (2003) 10–21 <http://www.smartcardalliance.org/alliance_activities/privacy_report.cfm>.

[218] Hong Kong is such an example. Until the enactment of the Hong Kong *Bill of Rights Ordinance 1991* and the Hong Kong Ordinance, there was no real respect for information privacy. The enactment of the Hong Kong Ordinance, pursuant to which an independent Commissioner was appointed and supported by the Office of the Privacy Commissioner for Personal Data (an independent statutory body), and the extensive education of the Hong Kong citizenry as to their information privacy rights, has resulted in the increased demand for protection of information privacy in Hong Kong: Letter from Stephen Lau, Privacy Commissioner for Personal Data, 4 August 2001, in Office of the Privacy Commissioner for Personal Data, Hong Kong (2001) 8 *Private Thoughts* (Newsletter) <http://www.pco.org.hk/textonly/english/publications/

If, however, the enacted personal data protection legislation is substantively the same as the current draft PDP Bill, then it would appear that the true intention of the government in implementing the MyKad project is to enable 'Big Brother' to engage in the perpetual surveillance of its citizens, exactly as George Orwell predicted in his book *Nineteen Eighty-Four*. This would inevitably be counterproductive to the various aspects of 'development' incorporated within the Malaysian government's 'Vision 2020'.[219] Without a proper legal framework for the protection of personal information, the MyKad will become the 'one card to rule them all'.

newsletter_issue8.html>. It was only after the establishment of a proper legal framework for the protection of personal information and the infusion of self-awareness of information privacy rights that the Hong Kong government attempted to implement a multipurpose Smart ID Card in 2003. Yet, as a result of intense objections from the Office of the Privacy Commissioner for Personal Data and the citizens of Hong Kong, the Hong Kong government has backed down on a number of proposed applications for the Smart ID Card such as the driving licence, health information and bank records, and the amount of information to be contained in the ID Card has been drastically curtailed. The Smart ID Card will now be limited to only basic uses: Mark Landler, 'Fine-Tuning for Privacy: Hong Kong Plans Digital ID', *The New York Times* (New York), 18 February 2002, C4; '"Smart" ID Card Worries Hong Kong', *Wired News* (Hong Kong), 10 March 2002 <http://www.wired.com/news/print/0,1294,50961,00.html>.

219 See above n 6 and accompanying text.