JIS

How much is too little? Privacy and smart cards in Hong Kong and Ontario

Stuart G.M. Bailey

Collaborative Program: Faculty of Information Studies/Knowledge Media Design Institute, University of Toronto, Canada

Nadia Caidi

Faculty of Information Studies, University of Toronto, Canada

Received 25 September 2004
Revised 9 March 2005

Abstract.

In this article, we analyze the notion of privacy – how it is conceptualized and implemented as a constitutive element of identity – in two different cultures: Hong Kong, a Special Administrative Region (SAR) of the People's Republic of China (PRC), and Ontario, Canada. By examining the two jurisdictions of Hong Kong and Ontario, we argue that, in addition to institutional structures, differing cultural notions of privacy affect the acceptance of new information and communication technologies (ICTs). For our comparison, we focus on one potentially privacy-invasive technology, smart cards, and discuss the factors that contribute to their adoption and use in the two regions selected, including one's conceptualization of digital identity and privacy, and the role of consultation and public debate.

Correspondence to: Nadia Caidi, Assistant Professor, Faculty of Information Studies, University of Toronto, 140 St George Street, #646 Toronto, Ontario M5S 3G6, Canada. E-mail: nadia.caidi@utoronto.ca

Keywords: privacy; technology; anonymity; government; Ontario; Hong Kong; smart card; consultation; digital self

1. Introduction

> New information technology disintegrates national borders; international traffic in personal data is a central feature of commercial life. [1]

In the contemporary landscape, where information and communication technologies (ICTs) are widely used by business and government, data travel around the globe nearly instantaneously. This creates certain considerations for an individual's identity: will personal information collected in one location be used in a consistent manner while in another? Will an individual's personal data be subject to different laws depending on where his or her digital footprint lands? Why should it matter at all whether there is congruency across jurisdictions [1]?

The nature of transborder data flow means that data protection legislation must take into account these questions of privacy. Contiguity of data protection across national borders is problematic at best, despite international efforts to provide a common ground. Moreover, the adoption of new technology, such as smart card technology, may be affected by cultural assumptions, values and attitudes towards identity and privacy.

Concepts of privacy and identity do not cross borders as effortlessly as data about an individual do. The presence and use of ICTs forces us to consider the relationship between an individual's identity and privacy in new terms. Relying on a single, static notion of privacy may do more harm than good as we

collectively move from paper-based information management into digital information management. Privacy is a contextual concept; its interpretation changes based on the environment in which the concept is engaged. The ability to manage personal borders in changing environments helps us distinguish ourselves from others, and enables us to manage our own identities by exerting some degree of control. Privacy is the interest that is engaged when those borders are breached. Remedies help us to recover from these breaches, the same way clothes may offer a remedy for nakedness. In the domain of personal information, breaches occur when an individual's personal information is used without that person's knowledge or consent, especially when used for an unreasonable purpose. To mitigate these risks, policy and law makers turn to an international set of fair information principles, which are used to guide the use of personal information so that breaches are minimized.

As privacy has moved from a relatively simple 'right to be let alone' [2] towards a right to informational self-determination [1] over data about oneself, it has become, in the words of one observer, 'a frustratingly protean concept' [3]. Management of one's identity has become equally challenging. Individuals must not only guard against the use and disclosure without consent of their personal information, but also its collection. Over the past decade the rise in identity theft has been meteoric. It is now one of the chief concerns of law enforcement and a major problem for government-issued identification; in 2004 the US Federal Trade Commission reported that identity theft affects 10 million citizens annually, and accounted for $52.6 billion in costs accrued by business for 2004 alone [4].

In this article, we examine the notion of privacy in Hong Kong, a Special Administrative Region (SAR) of the People's Republic of China, and Ontario, Canada, two jurisdictions that have similar data protection frameworks and a similar level of consumer acceptance for new technology. By doing so, we argue that (other things being equal) government-initiated consultation plays an important role in developing a comprehensive, practical and shared concept of privacy, which allows us to navigate the changing digital landscape. While we do make references to private sector implementations of smart card technologies, the focus of the article is on the role of public sector consultation and how it affects the development of a shared concept of privacy. We examine how this shared concept affects the adoption of new and potentially privacy-invasive technologies like smart cards. Our findings indicate that, in an age of increasing sensitivity towards privacy concerns, smart card initiatives must be open and transparent in both the design of the architecture and the consultation process with users in order for the new initiative to be embraced.

2. Framing privacy in Hong Kong and Ontario

Privacy has been addressed by many before us and yet it continues to evade a concise definition. Some conceive of privacy as having four 'dimensions': privacy of the body; privacy of personal behaviour; privacy of personal communications; and privacy of personal data, also known as informational privacy [5]. Despite the criticism that doing so risks invoking an antiquated conceptualization of privacy, we refer to the elements of privacy as articulated by Alan Westin's seminal book, *Privacy and Freedom*. In it, Westin proposes four categories that help us apprehend the concept of privacy: solitude, intimacy, anonymity and reserve [6]. Westin's conceptualization of privacy remains compelling in part because it allows us to examine an issue that remains sensitive in many countries: anonymity. Anonymity is the ability to remain unnoticed in public. North America continues to show some sensitivity to this issue in particular. Half a century after introducing the concept in his book *1984*, George Orwell's 'Big Brother' continues to evoke strong feelings and makes regular appearances in books, movies, radio, and television when describing the power of the state [7, 8]. The war on terror waged by the US (and other countries) has also contributed significantly to the impression that the state will exercise powers which are only weakly curbed by civil rights. Moreover, as we found in our research, many Hong Kong government documents use Westin's language. We feel that this provides a meaningful link between Eastern and Western conceptions of privacy and it is particularly relevant to our examination of shared understanding of 'privacy' in that anonymity is curiously absent from definitions of privacy in Asian culture.

2.1. Hong Kong

Whereas in Ontario there is a fairly well established tradition of privacy concerns both in law and in culture, there are conflicting opinions about the prevalence of privacy in traditional Chinese, and by extension, contemporary Hong Kong culture. One

privacy commissioner for Hong Kong indicated that protection of personal data in Hong Kong is a matter of culture and that Chinese people have not historically possessed a strong concept of privacy [9]. Privacy as a term is relatively new: interestingly, the characters that altogether form the concept of data protection are 'hide', 'private', and 'right'. While it is true that data protection and privacy rights are relatively new, studies show that privacy is nevertheless in the top five concerns of citizens in the region [10].

When it comes to privacy, Hong Kong citizens' conceptions of privacy seem to share the qualities of solitude, reserve, and intimacy enunciated by Westin [6] in 1967, but seem to differ with regard to the cultural desire for anonymity that seems to be more prevalent in the West [11]. Chan's excellent review of familial privacy in Hong Kong shows that there are empirical data to suggest the nuclear family unit is the centre of individual privacy for Hong Kong citizens, something that differs from the Chinese model where the extended family is included in the familial sphere [11]. As Chan notes: 'Only anonymity, the capability to remain unrecognized in a public [sic], does not apply to the Chinese conception of privacy. The reason for this is that anonymity has never been regarded as a problem in Chinese society because people prefer to be recognized and praised for their conduct or achievements by fellow clansmen and neighbours' [11, p. 2].

While Liang [12, cited in 11, p. 15] argues that the Chinese have not had concepts of privacy rights and freedoms in the past, Chan points out that Hong Kong is situated between the Chinese model and the Western model, and shows that 'individual rights of privacy are subject to one's status within a social group' [11, p. 5]. Other sources show that the 'right to privacy' as a means of protecting personal interests is ambiguous in Chinese society and that the Chinese define 'public' and 'private' in abstract ethical terms [13], thus leading Fahey to note that the 'interpretation of privacy is culturally specific' [14, cited in 11, p. 2]. To Chan, however, 'zones of privacy' (such as privacy and boundaries in the family) are 'culturally specific to context, and . . . are believed to be constantly defined and redefined in relation to trends in social change.' In the Hong Kong concept of privacy, these zones are managed through asymmetric relationships (e.g. king–vassal, father–son, husband–wife), and

> the dominant in a dyad relationship can acquire the information he/she wants from the other party because it is considered justifiable and natural to do so. A reversal of this is an offence. Therefore, individual rights of privacy are subject to one's status within a social group. [11, p. 5]

When conceived of in these terms, invoking privacy interests as a means for protecting rights to informational self determination seems odd to a Western eye, because it seems to be an ineffective means of exerting one's control.

The variance of cultural and lifestyle norms indicates that individuals' preferences and social habits may play a part in determining how comfortable that person is in embracing new technology [15]. The cultural values held by a group also play a significant role in the adoption of new technologies. The developments in e-commerce, for instance, build on the trust factor inherent in many transactions, along with the long-standing tradition of bargaining. Indeed, Chinese culture relies heavily on the socialization effect of on-site commerce (i.e. friendly conversations between the vendor and the customer), which encourages business success through the quality of personal relationships [16].

Similarly, the fact that Hong Kong is so far ahead of Ontario in its acceptance of smart card technology seems to be supported by the fact that the notion of anonymity is not as prevalent in the Hong Kong notion of privacy. Cultural and lifestyle norms in Hong Kong do not invoke anonymity as strongly as elsewhere – for example, Ontario – and so the adoption of smart card technology may have one less hurdle to overcome.

Residents of Hong Kong have had to carry immigration-related identification since the late 1940s and the government of Hong Kong is currently in the process of re-issuing the existing cards with a multi-application smart card called the Hong Kong Smart ID card (HKID) [17]. The government plans to have the re-issue complete by 2007. The card will be used for immigration purposes but also has non-immigration applications such as e-Cert (electronic certification for virtual transactions), library card, and driving license-related functions (the last being planned for around 2006). The presence of non-immigration applications on a government-mandated identification card has raised privacy concerns amongst citizens of Hong Kong [18], and so as part of its implementation, the government undertook a consultation process in order to ease the smart card into general use. The government has acknowledged that privacy is important to citizens of Hong Kong and has taken steps to demonstrate compliance with Hong Kong's privacy legislation and best practices. As an example of its policies of openness, the government posted the Privacy Impact Assessment for smart cards on its website. The consultation process was intended to help the adoption of smart cards by providing citizens with a common language to address

mutually held concerns. In turn, this allowed individuals gradually to reach a collective understanding of the issues created by the uses of these new technologies. A common language is helpful in identifying and framing concerns. Consequently, the common language established a familiarity with the issues, and in turn eased the adoption of technology – even though that technology may be privacy-invasive.

The process of consultation helps build this common language for privacy concerns. By virtue of the consultation process taking place, citizens in Hong Kong have had the opportunity to engage collectively in a common discourse about privacy rights. The government has provided details about the architecture of the system, and has made public statements about what they will and will not do with an individual's personal information. Given that Hong Kong has adopted smart cards so widely, and Ontario has a more cautious attitude, one can wonder about the extent to which socio-cultural factors affect the adoption of new technologies such as smart cards.

2.2. Ontario, Canada

A multicultural and modern society, Canada is one of the many countries in the world that has implemented data protection legislation. As with all other countries responding to the rapid growth of information communications technology, Canadians have been faced with integrating prevailing assumptions, beliefs and values with the emerging digital environment.

Despite the almost ubiquitous loyalty cards in the Canadian marketplace, Canadians have shown that they are disturbed when it comes to allowing an organization to track their activities, habits and personal information. Smart card initiatives in Canada have not been anywhere near as successful as they have elsewhere in the world (such as the Hong Kong's Octopus card). In the mid-1990s, Mondex, an electronic cash-replacement initiative run by MasterCard, was an illustration of this Canadian paradox. Although Mondex was not any more privacy-invasive than any other card, the gray zone between what kind of personal information would (or could) be collected and what an individual would have the right to control and protect was enough to create a climate of suspicion around the card's daily use. It was 'as if the technology was introduced primarily for the purpose of gathering more personal data' [19]. Similarly, an initiative in 2002 to develop the Ontario Smart Card (and its national equivalent in 2004) was met with an uproar. Greater transparency in the Mondex smart card technology would perhaps have helped its acceptance and adoption. As it was, the lack of transparency and accountability on the part of the system designers and owners of the technology (Mondex) prevented it from being embraced sufficiently to reach the stage of stabilization required for a new technology to be adopted – people simply did not trust it, and since they saw no reward for doing so, they let the idea die on the vine [19].

3. Legislative frameworks

The protection of privacy is addressed both in common law and in data protection legislation. Although common law approaches to privacy are not universal, they apply to Hong Kong and Canada, as both jurisdictions are heavily influenced by the British system. This article focuses on data protection legislation (common law issues as they relate to privacy can be found elsewhere [1, 9, 20]).

Data protection legislation in Canada and Hong Kong is guided by international principles and standards that have developed over the past few decades. The most important influences on the contemporary data protection discourse are based on:

(1) the Fair Information Practices;[1]
(2) the guidelines developed by the Organization for Economic Co-Operation and Development (OECD) in 1980 [21]; and
(3) the European Union's Data Directive of 1995 [22].

The latter provides a comprehensive framework binding member states and outlines the obligations of countries seeking to do business with European members [1]. These three standards are effectively the cornerstones of contemporary data protection legislation around the world. The OECD Guidelines are based on the fair information principles, which are intended to give an individual – within some limits, such as health or safety emergencies – a framework for the collection, use, disclosure, retention and disposal of personal information [23]. Canada and Britain are both member countries of the OECD.

As early as 1980 the OECD recognized that, although national laws and policies differed, there was a shared and compelling economic interest in facilitating the transborder flow of information while protecting privacy interests. The eight principles published in the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* are intended to level the playing field for those organizations – in both the public and private sectors – that handle or process

personal data [23]. These agreements were, however, introduced as much in the interests of enabling trans-border data flow as protecting privacy.

Both Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) and Hong Kong's *Personal Data Privacy Ordinance* (PDPO) function as 'privacy laws' by means of protecting against the unauthorized collection, use, or disclosure of personal data. Both also give individuals the ability to access their personal information, and both provide oversight through the establishment of a Privacy Commissioner. Whereas the PDPO applies to both the public and private sectors, PIPEDA applies to the commercial sector only, and is aided by a number of public sector statutes and regulations for the purpose of data protection in the public sector.[2] The PDPO

> covers any data relating directly or indirectly to a living individual (data subject), from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable. It applies to any person (data user) that controls the collection, holding, processing or use of personal data. [24]

PIPEDA applies to identifiable information about an individual, with some exceptions. One strong critique of Canada's legislation, however, is that it rests on a complaint-based system: in order for wrongs to be addressed under PIPEDA, an individual must know that

(1) there has been an infringement of personal privacy, and that
(2) certain kinds of complaints can be made to enforce compliance.[3]

But if Canadians are unable to determine that a breach of privacy rights has occurred, then they will not complain. If they do not complain, then there are no repercussions for those who infringe privacy. If there are no repercussions, there is little incentive to comply with data protection legislation (that is to say the repercussions may be so insignificant as to make not complying easier than complying). Because privacy rights have in many ways been born out of marketplace interests, government regulation is necessary to ensure a fair playing field for all competitors, the same as might be expected for other kinds of trade and commerce. Government has taken the first step of introducing data protection legislation and making the Privacy Commissioner an Officer of Parliament – a process that did involve consultation with privacy experts and industry leaders – but successful data protection legislation in Canada needs help from regular citizens. Just like Hong Kong, Canada needs a public discourse about privacy rights, a common language to identify issues and frame shared concerns. If individuals are able to identify the body that goes with their digital identity, they are also better able to negotiate or navigate its use or protection – better able to pick out its wardrobe, one might say.

4. 'Selling' the idea of smart cards: a comparative analysis

Hong Kong and Ontario share many similarities, such as an existing data protection legislation, a strong focus on the economy, an active press, and an involved research and academic community. Similarly, both Hong Kong and Canada have been considering smart card use at various points in time. Hong Kong has moved forward with such initiatives while Canada still falters in its implementation and adoption of smart card technology.

4.1. Diffusion of smart cards

Since their invention in 1974 by French journalist Roland Morentic, smart cards have been widely adopted in France, Spain, Holland (all of whom are world leaders in smart card use) and so on [25]. In 1998, Europe accounted for 73 percent of worldwide smart card use. According to industry analysts, Asia's growth in smart card use was expected to represent 24 percent of global markets by 2003. Growing from US$1.5 billion in 1999, the 2003 global market for smart cards was expected to be US$8 billion [26]. Smart cards are now found in GSM phone technology, satellite television receivers, student identification, casino e-cash, and multi-use identification badges.

Smart cards are plastic wallet-sized cards embedded with a computer chip capable of storing and retrieving information. Smart card technology can also serve as a verification device for identity management schema, or as an electronic wallet. The ability to connect a few databases and make smart cards a *de facto* surveillance tool is obvious. Smart cards are also tools of convenience, and their ease of use is a common reason for their adoption. But it is likely that there is more than one reason for a society to adopt the widespread use of smart card technology.

In Hong Kong, mobile commerce has emerged as a viable option for purchasing items without having to carry any cash. It has proved to be a very attractive option for making purchases. The ubiquitous Octopus card [27] is a metropass of a sophisticated nature.

Introduced in 1997, by 2000 there were 6.4 million cards in circulation performing 4.5 million transactions daily [28]. They can store over US$100, can be reloaded and the balance easily checked at add-value stations, and can be used on a networked system of retailers and services throughout Hong Kong. There are a number of factors that affect smart card adoption in Hong Kong, including ease of use, convenience, efficiency, reduction of clutter, better service, and e-commerce potential. As Ure notes,

> In a fast-paced, indeed hyperactive, society like Hong Kong consuming delay is regarded as a major inconvenience, especially during rush hours, so a premium is placed upon the immediacy of micro-payment where the item in question is routinely consumed with very high frequency. [29]

Taking advantage of this market is therefore a compelling business opportunity for Hong Kong businesses. The Octopus system has now made its way into 7-Eleven and Starbucks for micro-payments, and its radio frequency identification (RFID) technology is small enough to fit into special Octopus watches and rings. The system also connects 23 separate categories of service, from paying for laps at the swimming pool to gaining access to the workplace, to vending machines, cake shops, fast food, retail, and parking. With an annual growth rate of 5% GDP for the last 20 years, Hong Kong seems a likely market for the potential future use of smart card technology.

In Canada, the Mondex initiative was a similar attempt to introduce smart cards in Ontario from 1997 to 1998 [30]. Mondex, however, was never successfully introduced in Ontario. A number of reasons were advanced to explain this failure: the prohibitive cost of entry that provided little demonstrable benefit to users; a lack of interest from consumers that translated into disincentive for merchants; and the general lack of interest from users who did not buy into the idea. Some suggest that these combined factors led to the abandoning of the Mondex initiative [19]. Other sources indicate that Mondex's failure in the marketplace was a result of a lack of sustainable financial backing [30]. Ultimately, the Mondex initiative seemed to have failed to engage consumers sufficiently with a valuable product that could convince them to adopt it for regular use. It is interesting to note that at the exact same time as consumers in Ontario were rejecting the Mondex card, Hong Kong was seeing the introduction of both the government's Hong Kong ID card and the Octopus card: within the first eight weeks of being made available, the population of Hong Kong had snatched up two million cards – 16 times the number of Hong Kong passports [31]. In 1998 Master Card International reported that, since its introduction in late 1997, 110,000 customers in Hong Kong had applied for Mondex cards, and that 6000 merchants were already on board [32].

Technologies such as smart cards have the ability to collect, store, and recall large amounts of personal data. Misuse of personal information presents a threat to adoption of smart cards because it represents a loss of ability to control one's personal information. Overcoming this hurdle (e.g. by negotiating this tension between convenience and privacy) is essential if one is serious about 'selling the idea' of the smart card and eliciting interest from potential users – something neither the Mondex nor the Ontario government's Smart Card Project ever succeeded in achieving.

In Hong Kong, various claims of adequate privacy protection have been made:

> Smart cards, with on-card intelligence and processing capabilities, are uniquely capable of enabling compliance with strong privacy guidelines and of enforcing the privacy and security policies [set by the health care organization]. Smart cards can protect personal information that is on the card, provide authenticated information access, and authenticate the legitimacy of other components during a transaction. When used appropriately and correctly, smart cards are the most privacy-protective of any ID card technology and provide unique features that both improve the system's security and protect the individual cardholder's privacy. [33]

These and other bolder claims – for example, that smart cards will reduce fraud or enhance security – are looked on with cautious scepticism by the privacy community. While it may be true that smart cards offer enhanced security features, security does not equal privacy. Privacy is indeed contextual: the application of its protective principles must involve a judgement call on behalf of the person controlling the information.

4.2. The role of consultation

Much can be learned from examining the role of consultation in the process of informing users about smart card technology leading up to its adoption. We examined newspaper articles, published reports, conference proceedings, industry statistics, promotional material, and information published by government to assess the differences between Hong Kong and Ontario's approach to consulting with the public when introducing smart cards. Our findings point toward the potential of a well-conducted consultation process in

enabling a common language to identify privacy concerns. An open and informed public debate has the advantage of focusing the attention of a large user base on a particular discourse – privacy – and can help initiate the dialogue needed in order to develop a common language for privacy interests. Once this common language is adopted by a potential user base, the introduction of new technologies like smart cards may not seem as foreign or threatening to users because they have more access to information about the potential and the pitfalls.

4.2.1. Consultation in Hong Kong. From 1996, when the Basic Law of Hong Kong was reformed to bring in the PDPO [1], to a conference in 2002 at the University of Hong Kong organized by the Hong Kong Centre for Comparative and Public Law, the government in Hong Kong has shown its efforts to be open and transparent about the use of smart card technologies. The subcommittee for research on the PDPO received 80 submissions by various special interest groups such as the Consumer Council, the Journalists Association, the Society of Accountants, the Association of Banks, and the Direct Marketing Association [1]. The 2002 Hong Kong University forum – convened to discuss the ROP (Registration of Persons) Amendment's provisions among other smart card issues – was attended by government officials, privacy scholars, lawyers, researchers, and human rights advocates. The government's presence at conferences such as these, the publication of material on its website addressing privacy concerns, and the active part it took in the smart card debate in Hong Kong's media[4] point to the multiple attempts to engage the public on privacy and smart card issues.

Many criticisms of the smart cards in Hong Kong were expressed in the public discourse. Evidence of this can be seen in conference materials, journal articles, news media, and government communications. The Privacy Commission, for instance, indicated its concern for the security of the personal information while in the care of the HKID initiative. Security, the Privacy Commissioner has argued, is not synonymous with privacy and security provisions do not necessarily address all aspects of privacy [9]. The contextual nature of privacy was raised, particularly with regard to provisions that facilitate an individual's information self-determination. A prominent voice in the Hong Kong debate, Graham Greenleaf, made a submission to the Privacy Commissioner about concerns that use of the proposed non-immigration applications of the card was not voluntary [35, cited in 9]. Greenleaf went on to note that, because there was no Privacy Impact Assessment planned for the card, it was likely that the use of the card by private sector organizations would slowly creep in to the government-mandated system. Concerns about the 1997 hand-over of control of Hong Kong from Britain to the People's Republic of China were also raised as areas of concern over the governance of the card regime.

To these criticisms and concerns, the government replied that the technology was still untested, which meant that it was difficult to produce an assessment on its impact on privacy interests [9, 35]. However, in response to public concerns, the government altered the smart card's planned applications [9]. Measures were taken to:

(1) limit the amount of personal information stored on the card itself, and ensure the storage of personal data on back-end systems of those government departments concerned (i.e. personal information will not be shared indiscriminately between government departments);
(2) make the enhanced features of the card (non-immigration related applications such as a driver's license, library card, storage of digital e-Cert and change of address information) voluntary instead of mandatory; and
(3) limit access to personal information on the card or accessed through the card. Personal information stored on the card would be encrypted, and 'only authorized persons will have access to the data on the card' [34, p. 13].

Despite Hong Kong being a Special Administrative Region of the PRC, a factor from which one may conclude a lesser degree of democracy, Hong Kong's implementation of a smart card project has on the contrary proved to be open, transparent, and responsive to public concern and criticism. The Hong Kong government seemed forthcoming about hearing public concerns and addressing them in a transparent manner. The government responded to the concerns of the Privacy Commissioner by demonstrating changes to the information architecture for the project and attempting – within limits so as to preserve safeguards – to show transparency about the system's design [9]. The fact that such a debate exists may have contributed to raising the profile of privacy in the minds of citizens and potential users, which may have ultimately affected their understanding of the card's multi-application potential. The government's own consultation process has engendered this public discussion and, despite there still being many detractors and many concerns left to fully address, the fact that discussion

took place publicly provides a forum where regular citizens – those ultimately affected by what the card can do – have a voice in its adoption.

4.2.2. Consultation in Ontario, Canada. In contrast to Hong Kong, the Ontario Smart Card Project, which presumably took place in a North American setting, with its assumptions of broad and democratic participation, was shrouded in secrecy, in attempts to control the media, and a significant lack of administrative transparency [36].

The Ontario Smart Card Project (OSCP) was intended to be a multi-application smart card that would introduce and enable efficiencies in the delivery of government service. The card was intended to 'replace OHIP [Ontario Health Insurance Plan] cards, drivers' licenses, birth certificates, hunting and fishing licenses, and other cards that provide access to government services' [7].

Consultation for the Ontario Smart Card, which took place in 2000–1, was twofold: with industry groups and with the public. The former was instrumental in the government's process of developing a smart card strategy. The latter, although planned for in later stages of the project, never took place to any meaningful degree. In her comprehensive review of the Ontario Smart Card Project, entitled *Smart Card, Weak Effort?* Krista Boa [37] recounts the history and development of the OSCP. Through freedom of information requests spanning an entire year, Boa pieced together enough information to truly understand what the project comprised.

The process of consultation can take many forms: in the private sector, consultation can be considered as market research with focus groups; in the public sector consultation means canvassing the opinions of constituents in order to draft laws or policies that are representative of the wishes of the people [38]. Nevertheless, as Boa points out, 'For information to be useful in the consultation process, the OECD argues that it must be 'complete, objective, relevant, easy to find and understand' [37, p. 69]. Using the government's own documents Boa shows how the government sought to control the message about the card ('to maintain [a] reactive approach and low media profile' ostensibly aimed at the public so that government could assemble its background players from key stakeholders before 'going public' [37, p. 87]). Boa's work shows that the OSCP was anything but consultative.

Indeed, no documents for consultation with the public were released, although 'the project planned to conduct open public consultations in 2001 or 2002 based on a consultation paper that was to provide details about the card' [37, p. 92]. The OSCP was cancelled before public consultation could occur; consultation was planned for the later stages, and 'there is no evidence in the FOI documents and indexes that the consultation paper was drafted' [37, p. 92]. The opinion polling and surveying that did take place with the public was with less than 1000 people (in a province of 11 million). In fact, although the Ontario government at the time did plan to have a consultation process including a discussion paper, requests for feedback, and advertising of the consultation with a cover letter to all 'key stakeholders', the government actually tried to minimize the amount of information the public received. Despite not reaching the consultation phase because of the project's cancellation in January 2001, government documents obtained by Boa show that the government preferred a four-week circulation of proposals without public hearings because it would 'achieve[s] consultation goals . . . within a fairly controlled process and reasonable timeframe' [37, p. 107].

Taking this position put the government 180 degrees from advice given to it by privacy advocates, who argued that consultation should be done in the design phase, and that 'open, public consultation should occur after the project is capable of making available detailed information on the infrastructure design and the card architecture, as well as the PIA [Privacy Impact Assessment] results' [39, as cited in 37, p. 130]. Even the government's hand-picked pollsters reported from their surveys that 'the results distinctly show that increasing the public's access to information about the project and the technologies increases their level of confidence in the project.' Indeed, privacy advocates in Ontario argued at the time that 'The potential risks of smart card based systems to personal information privacy, predominantly in the form of increased potential for surveillance, warrant public consultation based on publicly available information about what is being considered and what is at stake' [39, as cited in 37, p. 137]. Furthermore, in the words of Roger Clarke, 'Public concerns about privacy-invasive and repressive applications of information technology must be reflected not only in the designs implemented by scheme operators, but also in policies implemented by governments' [40]. The Privacy Commissioner of Canada at the time himself said that he was 'not opposed to the use of smart-technology, just as long as the information it contains or access to it is sufficiently segregated and secured' [41]. Indeed, public consultation requires that the designers actually listen;

otherwise the process becomes 'political choreography' [42, cited in 37, p. 147]. The government committed itself on a number of occasions to the protection of privacy, but was never forthcoming about the technical aspects of the card. Biometrics were considered, but were deemed too contentious to proceed with [43].

Consultation has taken place at the federal level for PIPEDA (for which industry and special interest groups were primarily consulted), and for Canada's proposed National ID Card. And to be fair, the Ontario government did undertake extensive consultation for drafts of provincial privacy legislation – the provincial *Personal Health Information Protection Act* (PHIPA) being one result of this consultation process. The consultation process for the National ID Card in Canada was suspended and only ever produced an interim report [44], but reappeared periodically in the news [45, 46]. Ultimately, though, the legislatively mandated outreach functions of the Privacy Commissioners in Canada and the provinces notwithstanding, neither the provincial government in Ontario nor the federal government of Canada have meaningfully engaged the public in debate about the use of smart card technology.

5. Lessons learned

So, why is it that Hong Kong has such a high rate of adoption of smart card technology when Ontario does not? What accounts for such high use of this potentially privacy-invasive technology in one jurisdiction while in the other it is relatively unsuccessful?

Undoubtedly, there are many factors that come into play when considering early adopters of smart card technology (for example, convenience, reducing clutter in the wallet). However, cultural attitudes toward privacy (how people feel about it or how they make sense of it) and the nature of the public debates around it are, we argue, equally important to take into consideration. After all, technology is shaped by society and society in turn is shaped by it. Hong Kong and Ontario seem to have had different understandings of what constitutes privacy (for example, the importance of anonymity) as well as different experiences with the consultation process. The fact that the government in Hong Kong took active steps to engage the public in debate about smart card applications and to respond to its concerns by designing the technology in such a way as to demonstrate built-in transparency, accountability, and safeguards demonstrates the effects that such a consultation process can have. This interaction between public and government enhances the way that regular citizens understand how privacy works in their daily lives, lives that are very much entwined with the flow of personal data. In Ontario, relatively little dialogue between architects and users occurred, and in response the new technology was viewed with scepticism and distrust, leading to an anaemic public discussion about the consequences of using smart card technologies. The result has been a perceived lack of transparency and confusion in Ontario about the real motives and incentives for implementing and using smart card technology.

Since 2003, a Toronto-based company called Dexit has entered the marketplace. Dexit is an RFID-based contactless cash-replacement micro-payment program where users pay for anything up to $100 worth of transactions per day at fast food restaurants, drug stores, and coffee shops in downtown Toronto. By mid-2004, 32,000 users had signed up for an account. Dexit operated much like a pre-paid mobile phone, which makes the April 2004 deal between Bell Canada and Dexit for national distribution an interesting development. Have attitudes changed in Ontario since the failed Mondex initiative? Has there been sufficient public discussion about smart card technology to allow users to overcome scepticism and adopt their widespread use as Hong Kong has done? We will watch in anticipation over the near future to see whether things are changing in Canada. Future studies could focus on adoption rates and cultural attitudes towards privacy, and by so doing cast empirical light on the study of the elusive digital subject in Canada.

The process of broad public consultation is an important dimension of the development of a collective framing of privacy because it focuses attention and creates consensus on shared values, terminology, and understanding of protection measures (such as best practices or legislation). Consultation has the after-effect of providing a common base level for understanding the issues and the language. One pitfall for consultation is that it may be limited to specialists and subject-matter experts (in this case privacy experts), the general public not being actively engaged. However, government-initiated consultation may also have the effect of injecting increased transparency into the domain of specialists and making complex issues more accessible for public debate. (This may not be a responsibility that government necessarily wants, the Ontario Smart Card Project being one example of how a political initiative was unenthusiastically stick-handled through the province's bureaucracy.)

In this article, we have argued that citizens in Hong Kong have a better notion of what their digital

identities comprise. This, in turn, enables them to make more informed decisions about adopting smart card technologies. We acknowledge that this may not be the *only* reason, but with regard to privacy, it seems important to provide users with the information and knowledge to assess the potential and challenges that new technologies may have for one's personal information. Better informed decisions can then be made regarding the negotiation of one's personal boundaries or digital identities.

Acknowledgements

The authors would like to thank the following individuals for their comments at various points of the research for this article: Guy Herriges, Andrew Clement, Lisa Austin, Ian Kerr, Roger Clarke, Krista Boa, Adam Fiser, Rong Wu, Colin Johnston, The Toronto East Asia Library at University of Toronto, The Hong Kong Centre at the University of Toronto, and Adam Norman.

Endnotes

(1) See US Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens*, a Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare (now Health and Human Services), published by MIT Press in 1973.

(2) In Ontario, those that apply are the Freedom of Information and the Protection of Privacy Act R.S.O. 1990, c. F.31, the Municipal Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. M.56, and in the health sector, the Personal Health Information Protection Act. S.O. 2004, chapter 3, Schedule A; at the federal level: the Privacy Act R.S. 1985, c. P-21, and the Access to Information Act R.S. 1985, c. A-1.

(3) PIPEDA section 5(1) requires organizations to comply with the principles in Schedule 1; section 11(1) gives an individual the ability to file a complaint for a contravention of the privacy principles; and Principle 10 – Challenging Compliance gives an individual the ability to challenge an organization's compliance with the privacy protection principles in the Act.

(4) 'Our objective is to make use of the smart ID card to provide more convenient, user-friendly and value-added services and to drive the wider use of information technology in the community. There has been extensive public consultation and we are fully aware of the concerns expressed over choice and privacy' [34, p. 13].

References

[1] R. Wacks, Data privacy: reforming the law, *Hong Kong Law Journal* 26 (1996) 149–51.

[2] S.L. Warren and L.D. Brandeis, The right to privacy, *Harvard Law Review* 4 (1890) 193–220.

[3] R. Wacks, Privacy and anonymity, *Hong Kong Law Journal* 30(1) (2000) 177–83.

[4] Federal Trade Commission, *Identity Theft Focus of National Consumer Week* (2005). Available at: www.ftc.gov/opa/2005/02/ncpw05.htm (accessed 4 July 2004).

[5] Management Board Secretariat, Government of Ontario, *Privacy Impact Assessment Guidelines* (Queen's Printer, Toronto, 2001). Available at: www.gov.on.ca/mbs/english/fip/pia/pia1.pdf (accessed 6 September 2004).

[6] A. Westin *Privacy and Freedom* (New York, Atheneum, 1967).

[7] T. Boyle, Smart card chills privacy experts, *The Toronto Star* (15 January 2001) 06.

[8] F. Chan, Privacy chief warns of identity theft, *South China Morning Post (Hong Kong)* (4 March 2000) 2.

[9] R.C.Y. Chung, Hong Kong's 'smart' identity card: data privacy issues and implications for a post-September 11th America, *Asian-Pacific Law & Policy Journal* 4(2) (2003) 518–68.

[10] Q. Chan, New smart cards prompt serious privacy concerns, *South China Morning Post (Hong Kong)* (8 August 2000) 14.

[11] Y.K. Chan, Privacy in the family: its hierarchical and asymmetric nature, *Journal of Comparative Family Studies* 31(1) (2000) 1–17.

[12] S. Liang, *Zhongguo Wenhua Yaoyi* [The Essence of Chinese Culture] (Joint Publishing Company Limited, Hong Kong, 1987).

[13] Y. Jin, Zhongguo ren dui siyinquan de lijie [Chinese idea of privacy right], *Ming Pao Monthly* (February: 1994) 56–62.

[14] T. Fahey, Privacy and the family: conceptual and empirical reflections, *Sociology* 29(4) (1995) 687–702.

[15] Visa Research, Consumers say smart cards can revolutionize way to pay, *The Asian Banker Journal* (17 August 2001).

[16] A.M. Efendioglu and V.F. Yip, Chinese culture and e-Commerce: an exploratory study, *Interacting with Computers* 16(1) (2004) 45–62.

[17] Government of Hong Kong S.A.R., *Smart ID*. Available at: www.smartid.gov.hk/en/index.html (accessed 30 August 2004).

[18] C. Ong, Smart ID cards may cut time to track down disease; tagging technology touted as means of catching up with potential virus carriers, *South China Morning Post (Hong Kong) Technology Post* (8 April 2003) 1.

[19] F. Stalder, *Making Money: Notes on Technology as Environment* (PhD Thesis, Faculty of Information Studies, University of Toronto, 2001).

[20] L. Austin, Privacy and the question of technology, *Law and Philosophy* 22(2) (2003) 119–66.
[21] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). Available at www.oecd.org (accessed 5 July 2004).
[22] European Commission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities: Legislation* 281/23 (1995).
[23] OECD, *Guidelines Governing the Protection of Privacy And Transborder Flows of Personal Data*, Annex to the Recommendation of the Council, 23rd September 1980 Part II: Basic Principles of Application (OECD, Paris, 2002) 14.
[24] Office of the Privacy Commissioner for Personal Data, Hong Kong, *The Ordinance at a glance*. Available at: www.pco.org.hk/english/ordinance/ordglance.html (accessed 4 July 2004).
[25] M. Loh Ho-sang, High security spurs technology: Hong Kong lags behind in smart card savvy, *South China Morning Post (Hong Kong)* (5 December 1995) 14.
[26] S. Abrahams, Asia setting a smart pace in adopting card, *South China Morning Post (Hong Kong)* (29 June 1999) 5.
[27] Octopus Card website. Available at: www.octopuscards.com/eng/index.jsp (accessed 28 August 2004).
[28] P. Leung, Octopus enters fast-food shops, *South China Morning Post (Hong Kong) Business Post* (22 July 2000) 3.
[29] J. Ure, Mobile commerce in Hong Kong: a research paper, [presented to the] *E-Mob Research Conference, Center for Telecom Management, Davidson Conference Center, Los Angeles, CA., USA* (15 January 2003).
[30] S. Craig and R. Blackwell, Mondex pulls plug on Guelph pilot project, *Globe and Mail* (31 October 1998). Available at www.efc.ca/pages/media/globe.01nov98.html (accessed 29 August 2004).
[31] K. Sinclair, Octopus keen to stretch its tentacles, *South China Morning Post (Hong Kong)* (27 October 1997) 23.
[32] Overwhelming response to Mastercard's Mondex smart cards in Hong Kong, *Malaysia Economic News* (17 February 1998).
[33] Smart health cards: HIPAA and beyond, *Smart Card Talk* 9(8) (2004). Available at: www.smartcardalliance.org/newsletter/august_04/feature_0804.html (accessed 24 August 2004).
[34] C. Yau, Secretary of Information, Technology and Broadcasting, Access to personal data on smart card will be strictly controlled, *South China Morning Post* (25 January 2002). [Letter to the Editor]
[35] G. Greenleaf, *Summary submission concerning the "Smart" ID card and the Registration of Persons (Amendment) Bill, LegCo Paper No. CB(2) 2620/01–02(01)* (2002). Available at: www.legco.gov.hk/yr01–02/english/bc/bc56/papers/bc561011–2620–1e-scan.pdf (accessed 5 July 2004).
[36] T. Hamilton, 'Smart card' plan gets the scissors, *The Toronto Star* (22 January 2002) A04.
[37] K. Boa, *Smart Card, Weak Effort?: Consultation in the Ontario Smart Card Project* (MISt thesis, Faculty of Information Studies, University of Toronto, 2003).
[38] OECD, *Citizens as Partners: Information, Consultation and Public Participation in Policy-making* (OECD, Paris, 2001).
[39] A. Cavoukian, *Open Letter to David H. Tsubouchi, Chair of Management Board Secretariat* (2001). Available at: www.ipc.on.ca/english/pubpres/reports/mbc-0401.htm (accessed 15 May 2002).
[40] R. Clarke, *Chip-based ID: Promise and Peril* (1997). Available at: www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html (accessed 14 June 2004).
[41] T. Hamilton, Privacy abuses too easy with card; smart card rapped by Privacy Commissioner, *The Hamilton Spectator* (27 March 2001) D03.
[42] G. Cheeseman and H. Smith, Public consultation or political choreography? The Howard government's quest for community views on defense policy, *Australian Journal of Internal Affairs* 55(1) (2001) 88–100.
[43] A. Clement, Ontario's project on 'smart card' a bad idea, *The Toronto Star* (10 July 2001) A17.
[44] House of Commons Standing Committee, *A National Identity Card for Canada? Report of the Standing Committee on Citizenship and Immigration, Interim report October 2003*. Available at www.idsysgroup.com/ftp/cimmrp06-e.pdf (accessed 15 July 2004).
[45] J. Bronskill, Ottawa to issue digital passport, *The Toronto Star* (19 July 2004).
[46] J. Bronskill, I.D. proposals spark concern, *The Toronto Star* (6 September 2004).