Near-field Communication Technology: Regulatory and Legal Recommendations for Embracing the NFC Revolution

Allan Richarz[*]

INTRODUCTION

As a new workweek breaks over Tokyo, a young salaryman begins his trek to work. Cycling to the nearest train station, he leaves his bicycle in an automated bike lockup. Passing through the station ticket gate and into the crush of morning rush hour, the salaryman stops at a kiosk to pick up the morning paper, followed by bottle of water from a nearby vending machine. Arriving at his destination, he realizes he forgot to pick up *omiyage*, a traditional gift among Japanese co-workers, and stops at a bakery adjacent to his station before completing his commute to work.

Figure 1. Tap 'n' Go mobile phone NFC payment in Japan. Courtesy: CBC.ca

While just another day to a Japanese salaryman, this story is interesting in that over the course of his journey, the salaryman's wallet never once left his pocket. Rather, his payments were completed entirely by mobile phone; enabled by Near-field Communication (NFC) technology. Six kilometres, five transactions, and no wallet; this is the essence of *osaifu keitai*; digital e-wallets allowing instantaneous and convenient payments at the tap of a phone or other NFC-enabled device.[1]

---

* The author would like to thank Midori Otsu for her invaluable research assistance with this article. This article is the winning entry in the 2013 IT.Can Student Writing Contest.

1 Shiro Uesugi, "Consideration about successful introduction of smartcards: A comparative case study of Integrated Chip card business in Shikoku" (June 2007) 2:2 J of Entrepreneurship Research 96.

While well-established in Japan,[2] NFC, and the e-wallet mobile phone technology it enables, remains in its infancy in Canada.[3] It is, however, a technology that will one day be widespread in Canada, but one that also raises important privacy considerations, as well as regulatory and technical questions outside the ambit of this article, both in regard to the technology itself, and with the systems under which it operates.

Despite its ease and convenience, NFC technology raises a number of privacy issues. Chief among these concerns are the collection, retention, and usage of personally-identifying information contained within NFC-enabled devices by both private and public entities. Within that category, the most pressing privacy issues inherent in the collection and usage of such information relate to real-time tracking or after-the-fact habit profiling and identity theft. As well, privacy issues persist around the means used, if any, to secure and protect that information from unauthorized third parties both at the end-user and systemic database levels.

In light of these concerns, it is useful to examine the Japanese approach to NFC technology, both dealing with the physical technology itself, and the system of networks and databases in which that technology operates. Japan provides a strong model for comparison given the country's long-standing use of NFC technology,[4] and robust privacy-protection laws and industry guidelines which exist in relation to NFC usage. While privacy protection legislation exists in Canada, compliance is lacking and enforcement powers virtually non-existent for privacy commissioners. Amending Canada's privacy legislation by taking cues from the Japanese model will allow Canada to better anticipate, and embrace, the "e-wallet revolution".[5]

In that regard, Canada must update its privacy and criminal legislation, and provide clear industry guidelines in order to pre-emptively deal with expanded future uses of NFC technology. Such updates would include granting expanded powers to Canada's Privacy Commissioner to impose fines and orders on businesses found violating Canada's federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* [*PIPEDA*]. Hand-in-hand with expanded powers for the Commissioner would come binding regulations from the government for the NFC industry and stakeholders relating to data security and privacy standards, and updates to the *Criminal Code* specifically addressing electronic/smart-money payment cards through the addition of technology-neutral language. These changes, made before widespread adoption of NFC technology in the

---

2 Donald Amoroso & Remy Magnier-Watanabe, "Building a research model for mobile wallet consumer adoption: the case of Mobile *Suica* in Japan" (April 2012) 7:1 J of Theoretical & Applied Electronic Commerce Research 95 [Amoroso].

3 "Bankers group pitches cell phones as digital wallets" *CBC News* (14 May 2012), online: CBC News <http://www.cbc.ca/news/business/story/2012/05/14/mobile-banking-cellphone.html> [Cell phones as digital wallets].

4 NFC adoption began in earnest in Japan in 2002 with the introduction of the *Suica* transit payment system. See: "JR East launches its Suica system in Tokyo" (January 2002) 42:1 Int'l Railway J and Rapid Transit Review 18 [Suica System Launched].

5 Sam Gustin, "Paypal Pokes into POS 'e-wallet' market" *Wired* (30 April 2011) Online: Wired <http://www.wired.com/business/2011/04/figcard/>.

country, will allow Canada to proactively and effectively address concerns surrounding the technology and eliminate any "grey areas" in the law.

I. A BACKGROUND TO NEAR-FIELD COMMUNICATION TECHNOLOGY

(a) From RFID to NFC

Conforming to ISO 18092:2013,[6] Near-field Communication technology forms a subset of Radio-frequency Identification (RFID). Therefore, it is important to examine the functions of RFID in order to understand the operation of NFC technology.

RFID itself is a technology dating back to the Second World War, where it found use in Allied fighter planes as an early form of "Identify Friend-Foe" detection system.[7] In modern times, RFID technology is used across industries and society, primarily in relation to the tagging and tracking of livestock and inventory.[8] RFID, as critics of the technology are quick to point out, can also allow for tracking individual citizens.[9] As well, modern RFID continues to shrink in size; Hitachi's "mu-chip", for instance, is smaller than a grain of salt, earning it the nickname "smart dust".[10]

The technology behind RFID is relatively straightforward: a "tag" contains an antenna and microchip containing small amounts of identifying information. An external interrogator, or "reader", uses radio waves to pick up the tag's signal and retrieve the information contained within.[11] Of note is the distinction between "active" RFID tags and "passive". The former contains, in addition to its microchip and antenna, an onboard battery power supply, allowing for the active broadcast of its signal up to several hundred metres away. Passive tags, by contrast, rely on the external reader's radio signal to power the tag's antenna and microchip, necessitat-

---

6 See: International Standards Organization, *ISO/IEC 18092:2013 Information technology*, online: International Standards Organization <http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56692>. [ISO]

7 Office of Consumer Affairs, "Consumer Trends Report, RFID technologies and consumers in the retail marketplace" (Spring 2007), online: Industry Canada <http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02287.html> [Consumer Trends Report].

8 *Ibid.* at 3.

9 Kashmir Hill, "Court Rejecting Texas Student's Opposition To RFID Tracker Not As Outrageous As It Seems" *Forbes* (9 January 2013), online: Forbes <http://www.forbes.com/sites/kashmirhill/2013/01/09/court-rejecting-texas-students-opposition-to-rfid-tracker-not-as-outrageous-as-it-seems/> [Kashmir].

10 See: "RFID mu-Chip Products", online: Hitachi <http://www.hitachi.ca/Apps/hitachicanada/content.jsp?page=forbus/security/mu-chip/index.html&path=jsp/hcl/hcl/en/>.

11 Timo Kasper et al, "An embedded system for practical security analysis of contactless smart-cards", in D Savveron et al, eds, *The Proceedings of Workshop in Information Security Theory and Practices*, (New York: Springer, 2007), 151 [Kasper et al].

ing a much shorter read range.[12] NFC fits into this equation by having an intentionally short read range of 10cm or less away from a tag reader, and in many cases, requiring a read-range of 4cm or less.[13] It is important to note that while NFC can be considered short-range RFID, not all short-range RFID is necessarily NFC, as "short-range" RFID can still have a theoretical read range of 50cm or greater.[14]

(b) Applications of NFC Technology

Given the technology's short read-range, NFC is often incorporated into contactless platforms, such as access control badges or commuter passes. Examples of the latter include London's Oyster Card[15], Hong Kong's Octopus Card,[16] the Presto Pass[17] in Southern Ontario, and Tokyo's Suica Card.[18] NFC also forms the basis for e-wallet technology, which transforms commuter passes and mobile phones into contactless payment platforms across a number of different consumer contexts.[19]

As noted above, NFC technology is widespread in Japan, which makes the Japanese approach to the technology helpful in determining Canadian best practices. Driving the ubiquity of this technology is the "Super Urban Intelligent Card", or Suica, commuter pass and e-wallet.[20] Examining this particular card is useful in understanding the range of possibilities presented by e-wallet technology. Started in 2002 by the JR East Group rail company, Suica began as a contactless commuter pass designed to replace Tokyo's traditional, and expensive, paper-and-magnetic ticketing system.[21] Gradually, as engineers refined NFC technology further, Suica cards were embedded with electronic cash (e-cash) capabilities which allowed the

---

12 Office of the Privacy Commissioner of Canada, *RFID in the Workplace: Recommendations for good practices* (March 2008) 28, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/research-recherche/consultations/2008/rfid_e.asp>.

13 Michael David & Kouichi Sakurai, "Security issues for Contactless Smart cards" in Hideki Imai & Yuliang Zheng, eds, *Public Key Cryptography* (New York: Springer, 1998) 248 [Michael David]. See also: Kasper et al, *supra* note 11 at 158.

14 Yan Zhang & Paris Kitsos, eds, *Security in RFID and Sensor Networks*, (New York: CRC Press, 2009) at 157.

15 See Transport for London, "Oyster Online", online: Transport for London <https://oyster.tfl.gov.uk/oyster/entry.do>.

16 See Octopus, "Welcome to Octopus", online: Octopus Holdings Ltd <http://www.octopus.com.hk/home/en/index.html>.

17 See MetroLinx, "Welcome to Presto", online: MetroLinx <https://www.prestocard.ca/en/>.

18 See JR East Railway Company, "Suica", online: JR East Railway Company <http://www.jreast.co.jp/e/pass/suica.html>.

19 See Sony, "FeliCa", online: Sony <http://www.sony.net/pressroom/sonytec/FeliCa.html>.

20 JR East Management Planning Department, "20 years of JR East" (March 2008) 49 Japan Railway and Transport Review 21 [20 years of JR East].

21 Koichi Goto, "Passenger Service Technologies" (July 2000) 24 Japan Railway and Transport Review 51-2.

cards to be used as a micro-payment method at convenience stores, station kiosks, restaurants, vending machines, and department stores.[22] Several models of laptops in Japan are also equipped with an on-board Suica reader, allowing for the use of Suica cards in online purchases.[23] Further developments in the NFC field led to the above-mentioned *osaifu keitai*; NFC-enabled mobile phone e-wallets, which act as a digital Suica card.

While Suica cards utilize the same "tap and go" technique as payment methods found in Canada, such as Visa's Pay-wave,[24] these cards are distinct from credit and debit cards in that they are "stored-value" cards; that is, value is contained in the card itself, rather than linked through a bank or credit account.[25] Metrolinx's new Presto Card is similar to Suica in that it is also a stored-value card; however, Presto Cards can only be used, at present, in a commuting context without the broader shopping capabilities of Suica.[26] As the example of Japan shows, NFC technology is capable of allowing new digital forms of payment by transforming ordinary commuter passes and mobile phones into multi-purpose payment platforms.

II. PRIVACY IMPLICATIONS OF NFC TECHNOLOGY

NFC technology and e-wallets present a number of exciting technical innovations. Card read-times are less than one-hundred milliseconds and require no PIN input,[27] allowing for quick and easy transactions, as well as providing the convenience of a cashless micro-payment experience. The technology, however, does raise a number of important issues in relation to privacy as discussed below, which must be addressed in order to allow for the smooth and widespread adoption of NFC technology in Canada.

(a) Real-time Tracking: Fact or fiction?

Before analyzing realistic privacy concerns raised by NFC technology, it is necessary to first dispense with perhaps the strongest criticism of broader RFID technology as a whole: the spectre of real-time tracking of citizens through RFID

---

22 20 years of JR East, *supra* note 20 at 21.

23 See: The LaVie Z NFC-enabled laptop: Seamus Byrne, "Why you can't have the world's lightest ultra-book" *CNET* (7 September 2012) online: CNET <http://www.cnet.com.au/why-you-cant-have-the-worlds-lightest-ultrabook-339341473.htm>.

24 CBC News, "New credit cards pose security problem" *CBC News* (2 June 2010), online: CBC News <http://www.cbc.ca/news/story/2010/05/31/f-rfid-credit-cards-security-concerns.html>.

25 Amoroso, *supra* note 2 at 95.

26 Presto, "About Presto", online: Presto <https://prestocard.ca/en-US/Pages/ContentPages/About.aspx>.

27 Michael David, *supra* note 13 at 247.

by the state.[28] As a subset of RFID, NFC technology is not immune from this criticism. Critics such as former US Congressman Bob Barr allege that an individual carrying, or in more conspiratorial examples, surreptitiously implanted/affixed with, an RFID tag can be covertly tracked, in real-time, by government actors.[29] Numerous analogous contexts exist for this theory: RFID tracking of school children,[30] amusement park patrons,[31] and resort guests[32] are all realities. Without wading into the debate relative to RFID as a whole, however, the idea of real-time tracking of NFC devices is illusory.

It is important to recall the above discussion of active versus passive RFID and the operable read-range of NFC devices. NFC devices are passive and require power from the radio waves of an interrogator. Moreover, per their ISO standardization, NFC has a maximum read range of 10cm or less.[33] A theoretical doubling of that read range to 20cm would require that the power source to the interrogator increase sixteen-fold,[34] and the use of a "large copper tube antenna".[35] This presents two theoretical options for real-time NFC tracking: that a surveillant remain no more than 10cm from a target, which itself would obviate the need for electronic tracking, or that surveillance be conducted using massive, and conspicuous, interrogators, owing to the exponential power increases needed to read an NFC device from even two metres away. As American intellectual property expert John Eden notes, "critics of RFID technology often overlook or intentionally downplay the fact that extremely Orwellian RFID systems would require an integrated network of readers in addition to the ubiquitous affixation of tags".[36] Practically speaking, real-time tracking of NFC devices is not feasible and exists as a possibil-

---

28 Bob Barr, "Far more eyes are watching" *New York Times* (7 August 2011) online: New York Times <http://www.nytimes.com/roomfordebate/2011/08/06/is-it-still-possible-to-disappear/far-more-eyes-are-now-watching-than-hunted-db-cooper>.

29 *Ibid.*

30 Kashmir, *supra* note 9.

31 Brooks Barnes, "At Disney Parks, a bracelet meant to build loyalty (and sales)" *New York Times* (7 January 2013) online: New York Times <http://www.nytimes.com/2013/01/07/business/media/at-disney-parks-a-bracelet-meant-to-build-loyalty-and-sales.html?_r=1&hp=&adxnnl=1&pagewanted=1&adxnnlx=1357609868-eyqv65kWoRFF47O/45Xgfw>.

32 International Telecommunications Union, "Ubiquitous Network Societies: The Case of RFID" (April 2005), online: International Telecommunications Union <http://www.itu.int/osg/spu/ni/ubiquitous/Papers/RFID%20background%20paper.pdf>.

33 ISO, *supra* note 6.

34 Akshay Utlama Nambi et al, "Near Field Communication — Applications and Performance Studies" in KR Venugopal & LM Patnaik, eds, *Wireless Networks and Computational Intelligence, Volume 292* (Berlin: Springer-Verlag, 2012) at 9.

35 Kasper et al, *supra* note 11 at 158.

36 John M Eden, "When Big Brother Privatizes: Commercial Surveillance, the *Privacy Act of 1974*, and the Future of RFID" (2005) 20 Duke L & Tech Rev at 1, online: Duke Law & Technology Journal <http://www.law.duke.edu/journals/dltr/articles/pdf/2005dltr0020.pdf>.

ity only in theory. However, while real-time tracking may not be possible, there are legitimate concerns over NFC devices being used in ways contrary to the privacy interests of individuals.

(b) Profiling

NFC devices and e-wallets have long memories. Every purchase, train stop, and card top-up are dutifully recorded by an individual's NFC device.[37] This raises the very real possibility of companies building consumer profiles on its customers, especially in the case of NFC devices registered under an owner's name. This is, in fact, a reality with the Suica card. At the card's launch, JR East openly acknowledged that widespread acceptance of NFC payment by retailers was expected given the wealth of information it would provide on customers' traits and habits.[38]

The information provided to retailers can take many forms. An NFC device might reveal a person's favourite foods and stores, clothing preferences, alcohol consumption, and most frequently-ridden bus and train routes. Use of so-called "smart posters", which contain an NFC chip to provide a user with information on an advertised product, commonly movies, may also reveal film-watching habits, interests or other tastes.[39]

In one regard, this information may be used in a relatively benign manner as a means of market research. Stores, for example, could aggregate collected data to better understand which products sell well in their stores and which do not, and adjust inventories accordingly. This would be particularly useful to grocery stores which have large amounts of perishable goods.[40] A more intrusive use of collected data, however, would involve targeted advertising. If an individual was known enjoy a certain type of candy bar, a retailer could strategically place NFC readers in near the check-out counter to "push" advertisements for said candy bar or other impulse items to his customer's mobile phone. In-store digital television advertisements could similarly adjust to present advertisements aimed at customers currently in a given store.

(c) Personal Safety

In addition to recording an individual's shopping habits, NFC devices can be used to examine where an individual has traveled. In that regard, by examining

---

37 Ann Cavoukian, "Privacy by Design . . . Take the Challenge" Information and Privacy Commissioner of Ontario, at 169, online: Information and Privacy Commissioner of Ontario <http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf> [Privacy by Design].

38 Suica System Launched, *supra* note 4 at 19.

39 Ann Cavoukian, "Mobile Near-Field Communications: 'Tap 'n Go': Keep it Secure and Private" Information and Privacy Commissioner of Ontario at 5, online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf> [Tap n Go].

40 Shino Koda, "Towards Environmentally-friendly Management at "Konbini": Case study at a Convenience Store in Japan" (2012) 3:4 J of Alt Perspectives in the Social Sciences 950.

entrance and exit times at train stations or on bus routes, it is easy to determine a person's commuting habits, and consequently, where an individual may be at a given time based on those habits. Determining the general location of an individual's residence is also possible.

Media reports from Japan shed some light on practical applications of this principle. While the Suica system has never experienced a leak of personal data, there have been a number of cases involving the stalking of train passengers by railway employees.[41] By scanning a commuter's card while in an official capacity,[42] a station employee can examine the travel history and generally predict where and when a commuter will get off the train at the end of her workday. A passenger's Suica travel history can also be used in legal proceedings against a defendant.[43] London's Oyster card has a similar vulnerability. In one well-known example, a man's wife was able to enter his Oyster card serial number online to determine which stations he had visited. The husband was subsequently found to be carrying on an illicit affair, and his Oyster card travel history was tendered as evidence in the subsequent divorce proceedings.[44]

(d) Protection and Loss of Personal Data

Ontario's Privacy Commissioner, Dr. Ann Cavoukian, describes NFC as a "promiscuous" technology; that is, it provides unencrypted data to any reader within range, often without any authentication procedures.[45] No special technological know-how is required to read such a device. The Google Play Store is rife, for instance, with applications ("apps") for NFC-enabled phones which allow them to read the unencrypted data on NFC-enabled credit cards and commuter passes such as Visa, Suica, and Oyster.[46] While the "secure element" of a card requires more advanced knowledge to access,[47] an easily downloadable app can provide an individual with a credit card's number, account holder name, and expiry date, or a commuter's name, phone number, and travel history — information which is not stored within the secure core.[48]

---

41 Yomiuri Shimbun, "Tokyo Metro staffer leaked Pasmo data" (17 April 2012) online: Yomiuri Shimbun <http://www.yomiuri.co.jp/dy/national/T120417004863.htm>.

42 Shinsuke Uriuhara, "Automatic fare collection system" (2003) 123:8 IEEJ Transactions on Sensors and Micro-machines 25, online: Physics Abstract Service <http://adsabs.harvard.edu/abs/2003IJTSM.123..271U>.

43 *Decision of Nagahashi, Okabe, Iida JJ*, Case No. 1446 (2006), First Saitama District Court (Criminal), 11 June 2007 at para 4., online: Courts in Japan <http://www.courts.go.jp/hanrei/pdf/20071031170422.pdf> [translated by author].

44 Steve Bloomfield, "How an Oyster card could ruin your marriage" *The Independent* (19 February 2006), online: The Independent <http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html>.

45 Privacy by Design, *supra* note 37 at 169.

46 Google Play Shop, online: <https://play.google.com/store/search?q=suica>.

47 Wayan Suparta, "Application of NFC Technology for mobile airline ticketing" (2012) 8:9 J of Comp Science 1237.

48 Google Play Shop, *supra* note 46.

The voluminous quantity of personal information gathered by NFC devices is enough to make a retailer or marketer salivate, and there may be a temptation to commodify personal information for sale to telemarketers and other advertisers. While not unique to NFC, the misuse or sale of personal information collected by retailers is worrisome given the insidious and invisible nature of the data collection.[49] Beyond the nature of the data collection, however, the traditional concerns of identity theft and privacy invasion surrounding the selling of personal information still exist.

(e) Lack of the Basics: NFC and data security

The above issues can primarily be traced back to a lack of "Basic Access Controls"[50] (BAC) over card data, such as encryption or password protection. This appears to be a common design problem with NFC technology and is not limited to just commuter passes and credit cards. When Belgium introduced its new RFID-enabled e-passports in 2005, European researchers discovered that the e-passports were completely lacking in even basic encryption; that is to say, the passports were entirely unencrypted.[51] Making matters worse, this first batch of passports had been earmarked for distribution to military, diplomatic, and business elites, who consequently travelled with entirely unsecured passports.[52] Regardless of the platform, the ease with which personal information can be obtained through NFC devices is generally indicative of poor design. While the "secure element" of a device remains tamper-resistant, so-called "Track 2" data is inadequately secured, leaving individuals vulnerable to data and identity theft, and creating significant privacy concerns.[53]

III. LEGAL AND REGULATORY APPROACHES TO NFC TECHNOLOGY

The above privacy concerns represent significant, but not fatal, issues in the adoption of NFC e-wallet technology. These issues exist at both the end-user stage, and on a systemic level; that is to say, there are challenges with both the physical NFC devices themselves, and issues with the infrastructure under which those devices exist. As will be discussed below, these concerns can be dealt with at both the legislative and regulatory level. Before analyzing potential solutions to the privacy challenges raised by NFC technology, however, it is necessary to examine the legislative privacy frameworks under which NFC operates in both Canada and Japan.

---

49 Tap n Go, *supra* note 39 at 6.

50 Gildas Avoine et al "ePassport: Securing international Contacts with Contactless Chips" in Gene Tsudik, ed, *Financial Cryptography and Data Security, Volume 5143* (Brussels: Springer Berlin Heidelberg, 2008) at 145 [ePassport].

51 *Ibid.* at 150.

52 *Ibid.*

53 Thomas S Heydt-Benjamin et al, "Vulnerabilities in First-generation RFID-enabled Credit Cards" *New York Times* at 3, online: New York Times <http://www.nytimes.com/packages/pdf/business/20061023_CARD/fc2007-submission.pdf> [Heydt-Benjamin].

(a) Japan

(i) Act on the Protection of Personal Information

Passed in 2003 and taking effect in 2005, Japan's *Act on the Protection of Personal Information* [*APPI*] is that country's leading legal document relating to individuals' privacy rights.[54] The *Act* lays out important responsibilities for both private and state bodies pertaining to the handling of personal information.[55]

Two important provisions within the *APPI* relating to private corporations handling personal information are Articles 15 and 16. These articles state that a corporation must declare its purpose in handling personal data through a public "purpose of utilization" document, and that any handling of personal information cannot deviate from that document.[56] Further, Article 24 of the *APPI* states that the following information must be made immediately available to consumers:

- The name of the business operator handling personal information,
- The Purpose of Utilization,
- Procedures to meet various disclosure requirements specified elsewhere in the Act; and,
- Any additional notice requirements as set out by Cabinet Order[57]

Informed consent among consumers is the chief factor at play. The *Act* later specifies that the purposes of utilization be publicly posted, or that consumers be notified promptly by other means (in order for the collection of personal data to be lawful). And in any event, the collection of personal data cannot be through "deception or . . . wrongful means".[58]

The *Act* also deals with personal information on a broader systemic level. Business operators are required to take any necessary steps towards the "prevention of leakage, loss or damage" of personal data, as well as any other "security control" methods necessary to ensure the protection of personal data held by the operator.[59] Concomitant with the above system-level control of personal data, business operators are further obliged to exercise "necessary and appropriate" control over employees with access to personal data to ensure security control of the data and to prevent misuse.[60] Business operators are also expressly forbidden from passing along consumers' personal information to third parties without the prior consent of the consumers in question.[61]

The importance of these provisions rests in affixing clear responsibility to the management and ownership of businesses to ensure personal information within its control is not misused at either a corporate or individual level, and mandating pro-

---

54 *Act on the Protection of Personal information*, Act No 119 of 2003, online: <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf> [*APPI*].

55 *Ibid.* at arts 4-5, 7.

56 *Ibid.* at art 16.

57 *Ibid.* at art 24.

58 *Ibid.* at art 17.

59 *Ibid.* at art 20.

60 *Ibid.* at art 21.

61 *Ibid.* at art 23.

tections be put in place to maintain the security of its personal information databases. Preventing disclosure of personal data to third parties in Article 23 of the *APPI* is also important as, in the past, Japanese businesses were apt to view personal information databases as commodities to be freely bought and sold.[62]

One noticeable difference between Canadian and Japanese privacy legislation is the public body responsible for overseeing, and enforcing, compliance with the Acts. In contrast to Canada, Japan does not have Privacy Commissioners; rather, the responsibility for ensuring compliance with the *Act* is delegated to a "competent Minister". In the context of privacy legislation, the competent ministers are the Minister of Health, [Labour] and Welfare, the Minister of Land, Infrastructure, Transport and Tourism, and any other minister so delegated by the Prime Minister.[63]

Enforcement of privacy legislation in Japan also differs from Canada, as, in contrast to the Privacy Commissioners in Canada who can only issue non-binding reports and recommendations,[64] the competent Ministers are empowered with escalating enforcement powers of advice, recommendations, orders and, ultimately, regulatory sanctions.[65]

Enforcement of the *Act* takes a graduated approach. Ministers are permitted to provide general pre-emptory "advice" to business operators relating to compliance with the *Act*, while Article 34(1) of the *APPI* states violations of the *Act* may result first in a ministerial "recommendation" that violations cease, and that certain measures be implemented to ensure future compliance with the *Act*. If the above recommendation goes unheeded, the competent Minister may order compliance with the *Act* and with any previously-recommended measures.[66] Where a violation is particularly serious, flagrant, or otherwise causes "serious infringement of the rights and interests of individuals", the competent Minister may bypass the recommendation stage and order immediate compliance with the *Act*, as well as ordering a business operator to take any other steps necessary to correct the violation.[67]

Competent ministers are also empowered to compel business operators to provide reports to the relevant minister detailing the operator's handling of personal information. Where business owners refuse to provide reports, or refuse to accede to ministerial orders relating to compliance with the *Act*, the operator is liable for a term of imprisonment with work, or to a fine.[68]

Japan's privacy legislation also provides for a non-judicial complaint resolution process, wherein an individual wishing to make a complaint may first seek redress from an "authorized personal information protection organization" tasked

---

62 Yohko Orito & Kiyoshi Murata, "Socio-cultural analysis of personal information leakage in Japan" (2008) 6:2 J of Info Communications & Ethics in Society 163.

63 *APPI*, *supra* note 53 at arts 35-36.

64 CBC News, "Data breach fines sought by privacy watchdog" *CBC News* (4 May 2011) online: CBC News <http://www.cbc.ca/news/technology/story/2011/05/04/technology-data-breaches-stoddart.html> [Privacy Watchdog].

65 *APPI*, *supra* note 54 at art 34(1).

66 *Ibid.* at art 34(2).

67 *Ibid.* at art 34(3).

68 *Ibid.* at art 56.

with handling such disputes.[69] Such organizations are authorized, upon receipt of a complaint, to investigate a business operator and request a response from a targeted business. Absent justifiable reason, such requests for response cannot be rejected by a business.[70]

The above oversight and sanctioning provisions of Japan's privacy legislation are both key to ensuring compliance with the *Act*. The legislation is not heavy-handed in its treatment of business operators that violate the *Act*, however. The Act is geared towards the smooth and expeditious resolution of disputes and in providing a graduated enforcement regime by granting ministers discretion in how to encourage a business operator to comply with the *Act*. This is in line with promoting the Japanese government's "ubiquitous society" agenda of widespread technological adoption throughout the country.[71] At the same time, provisions exist which give "teeth" to the legislation, and allow for the government to force compliance with privacy regulations, and impose further penal sanctions for violations of ministerial directives.

(ii) Joint governmental guidelines on the applicability of the APPI

Japan's privacy legislation is not the only means through which the government attempts to protect individuals' privacy and personal information. Industry and technology-specific guidelines are also published to provide additional guidance in terms of privacy and data protection. Relating to NFC technology, the Japanese Ministry of Internal Affairs and Communications [MIAC], and Ministry of Economy, Trade and Industry [METI] published its joint "*Guidelines for Privacy Protection with Regard to RFID tags*".[72] These guidelines provide valuable clarification regarding NFC technology, and RFID as a whole, as it relates to Japanese privacy legislation. In that regard, the guidelines are explicit that "the use [of NFC technology] shall be regulated by the Law for the Protection of Personal Information".[73] Further, Article 3 of the guidelines state that, prior to a transaction with a consumer, NFC/RFID-tagged products and devices be identified as such by retailers, and that information be posted regarding the types of data to be contained or collected within those devices and products.[74] These guidelines have the force of

---

69 *Ibid.* at art 37(1).

70 *Ibid.* at art 42(3).

71 Lara Srivastava & Akihisa Kodate, "Ubiquitous Network Societies: The Case of Japan", ITU Workshop on Ubiquitous Network Societies, (April 2005) at 6, online: International Telecommunication Union <http://www.itu.int/osg/spu/ni/ubiquitous/Papers/UNSJapanCaseStudy.pdf> [Ubiquitous Society].

72 Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, Government of Japan, "Guidelines for Privacy Protection with Regard to RFID Tags", 8 July 2004, online: Ministry of Economy, Trae and Industry <http://www.meti.go.jp/english/information/data/IT-policy/pdf/guidelines_for_privacy_protection_with_regard_to_rfid_tags.pdf> [Joint Guidelines].

73 *Ibid.* at art 1.

74 *Ibid.* at art 3.

law, and are part of the broader "Guidelines for Personal Information Protection Laws Concerning Fields of Economy and Industry" regulatory scheme undertaken by METI in providing guidance to industry.[75]

(iii) Penal Code

The Japanese *Penal Code* also weighs in on the issue of NFC technology in relation to e-wallets, specifying a penalty of 10 years in jail or a fine of up to 1 million yen for the unauthorized use, possession, creation, or other misadministration of an electronic payment card.[76] The unauthorized collection or "spoofing" of information contained within an electronic payment device, or attempts to do so, also attract a penal sanction of three years in jail or a fine of 500,000 yen.[77] Also of note is the broad definition of "electromagnetic record" in the context of payment cards. Rather than focus on the physical medium in which the data resides, the Japanese *Penal Code* takes a technology-neutral approach, defining such payment cards as any payment medium containing data which is: a) "unrecognizable by natural perceptive functions"; and b) capable of being read by a computer system.[78]

(iv) Summary of the Japanese approach

The approach of Japan to privacy legislation is both comprehensive and effective. Privacy legislation provides for basic protections of individuals' personal information, and allows for a graduated enforcement mechanism up to and including penal sanctions. Privacy legislation is augmented by periodic ministerial guidelines relating to new advances in technology. In the context of NFC technology, privacy legislation and guidelines are bolstered by stiff criminal sanctions imposed by Japan's *Penal Code*.

One may note the irony of Japan having such a robust privacy and personal information protection regime, given that the Japanese language lacks a native word for "privacy", and that traditional Western concepts of privacy generally remain antithetical to the Japanese collective culture.[79] It is true that Japanese privacy legislation is not driven purely by altruistic concern for the protection of individuals' personal data; rather, business efficacy plays no small part in Japan's embrace of a robust privacy regime. As noted in the pre-amble to Japan's *APPI*, the purpose of the legislation is the protection of rights of individuals "while taking consideration of the usefulness of personal information . . . in an advanced information and

---

75 Ministry of Economy, Trade and Industry, Government of Japan, "Personal Information Protection", online: Ministry of Economy, Trade and Industry <http://www.meti.go.jp/english/information/data/IT-policy/privacy.htm>.

76 *Penal Code* (Japan), Act no. 36 of 2006, online: <http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf> art 163-2 [*Penal Code*].

77 *Ibid.* at art 163-4(1).

78 *Ibid.* at art 7-2.

79 Yohko Orito & Kyoshi Murata, "Privacy Protection in Japan: Cultural Influence on the Universal Value", cited in, "Global ICT-ethics: the case of Privacy" (2008) 6:1 J of Information, Communication & Ethics in Society,: Meiji University <http://www.kisc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf>.

communications society".[80] Elements of this business efficacy approach are also evident in the above-mentioned ministerial NFC/RFID guidelines, which contain provisions encouraging businesses to engage in public awareness campaigns touting the benefits of RFID technology to consumers.[81] As mentioned above, this accords with the emphasis of the Japanese government on remaining a technological innovator, and adopter, which ultimately entails the aggressive promotion of technology throughout society.[82]

Regardless of the motivations behind their privacy protection regime, however, Japan's comprehensive and multi-faceted approach to privacy and data protection provides invaluable guidance for improving and readying Canada's privacy protection regime for the future widespread adoption of NFC technology. One notes that in over ten years of operation, Japan's most ubiquitous NFC technology, Suica and Suica-enabled mobile phones, have not suffered a single major breach of customers' personal data; it is an achievement due in no small part to the clearly-defined system of rules under which the technology operates.[83]

(b) Canada

(i) Personal Information Protection and Electronic Documents Act

Operative across the country,[84] Canada's main privacy legislation is the *Personal information Protection and Electronic Documents Act* [*PIPEDA*]. Applying to, among others, every organization that deals with personal information in a commercial context,[85] *PIPEDA* seeks to "govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information" and the legitimate needs of organizations to make use of this information in the course of business.[86]

As noted above, a main point of divergence between *PIPEDA* and Japanese privacy legislation relates to the government body in charge of enforcing the legislation and the enforcement powers available to those bodies. While enforcement responsibility in Japan rests with a number of cabinet ministers, Canada, at the

---

80 *APPI*, *supra* note 54 at art 1.

81 Joint Guidelines, *supra* note 72 at art 10.

82 Ubiquitous Society, *supra* note 71.

83 Amoroso, *supra* note 2 at 105.

84 To address division of powers concerns, provinces with equivalent legislation to *PIPEDA* may use their own legislation. To date, British Columbia, Quebec, Ontario (for health information), and Alberta all utilize their own legislation. See: *Personal Information Protection and Electronic Documents Act SC 2000, c 5*, s 26(2)(b) [*PIPEDA*], and Office of the Privacy Commissioner of Canada, "Questions and Answers regarding the application of *PIPEDA*, Alberta and British Columbia's Personal Information Protection Acts" (5 November 2004), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/resource/fs-fi/02_05_d_26_e.asp>.

85 *PIPEDA*, *supra* note 84 at s 4(1)(a).

86 *Ibid.* at s. 3.

federal level, takes an "ombudsman" approach,[87] wherein investigative duties under *PIPEDA* are vested first in the Privacy Commissioner, with the possibility of secondary recourse to the Federal Court.

Canada's Privacy Commissioner is empowered to receive and initiate complaints relating to breaches in the handling of personal information, and conduct investigations using a broad range of powers including the ability to compel witnesses and evidence, as well as a right-of-access to any place apart from residences.[88] Upon completion of the investigation, the Commissioner then tenders reports to the complainant and respondent organization detailing the investigation's results, along with any recommendations the Commissioner sees appropriate. As Ryerson University's Avner Levin notes however, the Privacy Commissioner does not "have a lot of teeth" as the office is not currently endowed with enforcement powers.[89]

One will note that recommendations tendered by the Privacy Commissioner are non-binding. In contrast with the competent Ministers of Japan, and indeed of other jurisdictions,[90] the federal Privacy Commissioner has no power to compel offending organizations to take corrective measures, nor does the Commissioner have the power to impose sanctions on those organizations. Unsatisfied complainants, upon receipt of the Commissioner's report, must instead seek redress from the Federal Court, per section 14(1) of *PIPEDA*. It is there that they may seek orders for compliance or compensation. The Privacy Commissioner herself may also, upon completion of her report, make an application to the Federal Court.[91] In that regard, Canada at the federal level lacks a "one-stop shop" for seeking redress in situations involving privacy breaches. This two-step approach has attracted criticism from the BC Civil Liberties Association [BCCLA], which notes the low-cost benefit of an ombudsman approach is obviated by the high cost of taking a case to the Federal Court.[92] The BCCLA report further notes that respondents are "free to ignore recommendations [of the Privacy Commissioner]" with the only consequences being additional complaints.[93] While the Privacy Commissioner has had notable successes,[94] a common complaint remains the lack of enforcement powers held by the Commissioner.

---

87 "Your Privacy Responsibilities" (February 2010) at 19, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/guide_e.pdf> [Privacy Responsibilities].

88 *PIPEDA*, *supra* note 84 at s 12.1(1).

89 Privacy Watchdog, *supra* note 64.

90 *Ibid.*

91 *PIPEDA*, *supra* note 84 at s 15(a).

92 Kirk Tousaw, "Securing Compliance, Protecting Privacy: The *PIPEDA* Enforcement Evaluation Research Project" BC Civil Liberties Association (March 2006) at 27-28 [BCCLA Report].

93 *Ibid.* at 57.

94 Office of the Privacy Commissioner, "Facebook agrees to address Privacy Commissioner's concerns" (27 August 2009) online: Office of the Privacy Commissioner <http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.asp>.

(ii) Behind the times: A lack of binding governmental guidelines for NFC Technology

Looking towards technology-specific regulations on NFC, Canada lags in terms of binding guidelines for the NFC industry in the implementation and usage of the technology. While Industry Canada has conducted background research on the technology,[95] it has yet to proffer binding industry regulations similar to those issued in Japan in regard to NFC. Such guidelines would not be unprecedented in Canada; the Competition Bureau of Industry Canada has previously published guidelines relating to e-commerce.[96]

It is not to suggest that there is no guidance from the government in regard to NFC; rather, that such guidance is only advisory in nature. Ontario's Information and Privacy Commissioner, Ann Cavoukian, has published a number of reports dealing with Near-field Communication and best-practices proposals for the technology. These proposals, which are only advisory in nature owing to the IPC's lack of jurisdiction over businesses in a non-health information context, exhort businesses to adhere to "Privacy by Design" principles in order to strike the best balance between consumers' data protection and business efficacy.[97] An addendum to the Canadian Government's *Code of Conduct for the Credit and Debit Card Industry in Canada* has also been proposed, which would cover mobile payments, although its coverage would be limited to "payments initiated by consumers that access a *deposit or credit account through a debit or credit payment network* through a mobile device at the point-of-sale" [emphasis added], thus excluding NFC mobile payments.[98]

The private sector has also weighed in on the issue in a non-binding fashion. There exists a voluntary best-practices guide created by the Canadian banking industry in 2012 as it relates to NFC technology.[99] This best-practices initiative is designed to pro-actively foster a "convenient, open, safe and secure [NFC] ecosystem supported by a standards-based operating framework" and covers the broad range of stakeholders in future NFC development.[100] While both this voluntary code of ethics and the Ontario IPC's guidelines provide useful guidance to busi-

---

95 See generally: Consumer Trends Report, *supra* note 7.

96 Competition Bureau, "Application of the *Competition Act* to Representations on the Internet" (16 October 2009), online: Industry Canada <http://strategis.ic.gc.ca/SSG/ct02500e.html> [Industry Canada Guidelines].

97 Ann Cavoukian, "Privacy Guidelines for RFID information systems" (June 2006) at 2, online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf> [RFID Privacy Guidelines]; Tap n Go, *supra* note 39 at 11.

98 Department of Finance Canada, "Consultation Paper: Addendum to the Code of Conduct for the Credit and Debit Card Industry in Canada to address Mobile Payments" (September 2012), online: Department of Finance Canada <http://www.fin.gc.ca/n12/data/12-106_1-eng.asp>.

99 Canadian Bankers Association, "Canadian NFC Mobile Payments — Reference Model" (May 2012), online: Canadian Bankers Association <http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf>.

100 *Ibid.* at 7.

nesses dealing with NFC, the inherent weakness in both is their non-binding nature. Like Canada's Privacy Commissioner, Ontario's IPC lacks the power under the province's *Freedom of Information and Protection of Privacy Act* to compel businesses to adopt best-practice proposals.[101] Further, while the banking industry's best-practices guidelines are thoroughly presented, they ultimately remain non-binding on stakeholders.

(iii) Canada's Criminal Code: Not meeting the reality of NFC micro-payments

A further weakness of the current Canadian approach to NFC technology is the *Criminal Code*'s lack of applicability, as compared to the Japanese *Penal Code* in relation to crimes dealing with NFC technology. While the *Criminal Code* contains provisions specifically on the topic of credit card fraud, those provisions are inapplicable to NFC-enabled smart cards. The *Criminal Code* defines a credit card at Section 321(a)-(b) as:

> Any card . . . or other device issued or otherwise distributed for the purpose of being used
>
> a) On presentation to obtain, *on credit*, money, goods, services or any other thing of value, or
>
> b) In an *automated teller machine* . . . or a *similar automated banking device* to obtain any of the services offered through the machine . . . [emphasis added][102]

Under the above definition, NFC-enabled smart-cards would be excluded by virtue of the fact that payments made through that medium are not "on credit", given that smart-cards carry their value on-board. Further, lacking a magnetic strip or "chip-and-pin" technology, NFC-enabled smart-cards are not interoperable with ATMs and similar banking machines. While the *Criminal Code* does not explicitly address the issue of NFC smart-cards, it is arguable that the fraudulent misuse of such cards may be caught by general *Criminal Code* provisions relating to electronic mischief and identity theft.[103] Without clear application to NFC payment devices, as found in the Japanese *Penal Code*, there is uncertainty about which, if any, provisions of the *Criminal Code* may definitively apply to crimes surrounding NFC devices. The provisions addressing electronic mischief, for instance, deal with attacks against, and interference with, computer data and consequently are of questionable applicability to NFC "spoofing" or cloning. Further grey areas exist in the above-mentioned government credit and debit card Code of Conduct, which appears to exclude stored-value payment cards much the same way the *Criminal Code* does.

---

101 CBC News, "Wine club suspends orders after LCBO privacy dispute" *CBC News* (30 November 2012), online: CBC News <http://www.cbc.ca/news/canada/ottawa/story/2012/11/30/ontario-wine-club-suspends-orders-lcbo-privacy-dispute.html>.

102 *Criminal Code*, RSC 1985 c C-46 s 321(a)-(b) [*Criminal Code*].

103 *Ibid.* at ss. 402.2(1) and 430(1.1).

(iv) Summary of the Canadian approach

Canada's privacy protection laws and *Criminal Code* are not necessarily weak in general. In the face of potential widespread adoption of a new and ubiquitous technology, however, Canada risks "leading from behind" in regulating privacy and criminal activity surrounding NFC technology through outdated and/or ineffective regulatory and legislative schemes. Uncertainty and grey areas in the law undermine business efficacy, but also have broader societal impacts. It would be unfortunate for a massive data breach of an NFC database, or a criminal fraudster duplicating hundreds of NFC smart cards, to go unpunished due to uncertainty in the law.

IV. APPROACHES FOR MEETING THE E-WALLET REVOLUTION IN CANADA

To address the above shortcomings in Canadian law relating to NFC technology, there are a number of proposals which will better position Canada to deal with the technology pro-actively and effectively. While a number of these proposals fall into the broader debate surrounding Canadian privacy law in general, they nonetheless also find particular relevance to NFC technology.

(a) A Technology-neutral Criminal Code amendment

In addition to binding industry regulations discussed below, amending the *Criminal Code* is another means by which Canada can prepare for the widespread adoption of NFC. An amendment to Canada's *Criminal Code* would pave the way for wider adoption and usage of NFC-technology by making clear the illegality of tampering with, copying, or otherwise causing the maladministration of an NFC-enabled device. Potential amendments include changing the wording of Section 321 of the *Criminal Code* to include a broader range of payment cards, rather than just credit cards. Such changes were made to the Japanese *Penal Code*, the provisions of which apply not just to credit cards, but "other cards [used] for the payment of charges", including electronically-encoded payment cards and stored-value media.[104] Such an amendment is also supported in Canada by the Canadian Bankers Association, which has published a white paper stating that the *Criminal Code* does "not capture all of the present or future payment methods that may be threatened by criminal activity" and that flexible, technology-neutral language is required.[105] As noted above, while it is arguable that the provisions of the *Criminal Code* dealing with fraud and identity theft may be sufficient to cover NFC-devices, adopting broader language to cover non-traditional payment media will remove uncertainty from the law. At the very least, by updating the language of Section 321 of the *Criminal Code* to include non-credit payment cards, the criminal law will move towards technology-neutral language to cover NFC smart-cards and future next-generation cards.

---

104 *Penal Code*, *supra* note 76 at art 163-2.

105 Bill S-4, *An Act to amend the Criminal Code (identity theft and related misconduct)* at 3 — CBA Submission to the Standing Committee on Legal and Constitutional Affairs (3 June 2009), online: Canadian Bankers Association <http://www.cba.ca/contents/files/submissions/sub_20090603_01_en.pdf>.

The argument can be made that the *Criminal Code* need not pre-empt, nor react to, potential flash-in-the-pan technologies that are discarded just as quickly as they are adopted. To that end, there are no guarantees that NFC will become widespread in Canada and may very well enter obsolescence shortly after emerging in the Canadian market. While a valid concern, NFC's performance in Europe and Asia shows it has sufficient cachet to be considered a viable technology in North America, particularly as it is a technological system, rather than a single product which consumers may or may not support.[106] Further, there is the general principle of drafting technology-neutral laws so that legislatures need not continually play "catch up" with technological innovations. In that regard, by updating language in the *Criminal Code* relating to credit card fraud, the law will cover any number of future media-based payment methods and not just those made by NFC smart-cards.

(b) Binding Guidelines on Data-protection and Security Measures

Binding regulations issued by Industry Canada for the NFC sector are one such way the Canadian government can make current its policies towards Near-field Communication. As noted above, Industry Canada, through the Competition Bureau, has exercised this power previously in relation to application of the *Competition Act* to cross-border online commerce.[107] By providing clear rules to NFC stakeholders, Industry Canada can forestall any grey areas in the law concerning the applicability of *PIPEDA* or the *Criminal Code* to the technology, while also offering pre-emptory guidance on best-practices for securing customers' personal information.

On a technical level, Industry Canada guidelines would be beneficial in establishing basic security benchmarks for NFC technology both systemically and on an end-user basis. As Dr. Cavoukian notes with some frustration, many of even the largest and most sophisticated databases containing personally-indentifying information lack basic safeguards.[108] NFC devices themselves also remain vulnerable. While transactional functions of a smart card, for instance, are stored within the "Secure Element" of the card, information such as the card's serial number, travel history, and other personally-identifying information remain in unsecured plain text form, as noted above.

Potential industry security mandates on the end-user level could include basic encryption for NFC-enabled devices such as smart-cards and mobile phones that protects the totality of the information contained within, and not merely the "Secure Element". On a design level, NFC-enabled mobile phone apps should be programmed to only broadcast signals upon specific request of the owner, rather than being in an "always on" state.[109] Mandatory issuance, promotion, or integration of inex-

---

106 Cell phones as digital wallets, *supra* note 3.

107 Competition Bureau Canada, *Application of the Competition Act to Representations on the Internet* (16 October 2009), online: Competition Bureau Canada <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/RepresentationsInternet2009-10-16-e.pdf/$FILE/RepresentationsInternet2009-10-16-e.pdf>.

108 Privacy by Design, *supra* note 37 at 280-281.

109 Kasper et al, *supra* note 11 at 159.

pensive quick-access "Faraday Cages", which block RFID/NFC signals, is another possibility and current practice in U.S. e-passport issuance.[110] In Privacy by Design parlance, the preference should be for solutions that are "baked in" at the design level, rather than "bolted on" afterwards.[111] There is strength, however, in baked-in measures supplemented by bolted-on security features — for instance, a secure smart-card carried inside an after-market Faraday Cage.

On a systemic level, applicable beyond NFC-specific technology, basic encryption and passwords for databases must be mandated by industry-specific guidelines. While such measures will not deter a concerted attack by professional hackers, such basic steps will at least deter casual or opportunistic attacks against databases. System-side security measures cannot ignore the human factor, however. As Dr. Cavoukian reports, 70% of data breaches are attributable to insiders.[112] A significant number of data breaches can also be attributed to poor, or non-existent, database-handling procedures. Dr. Cavoukian further notes example after example of laptops, hard-drives, and other media containing the personal data of millions of individuals carelessly left on street corners, public transportation, and other similar locations.[113] To prevent, or lessen the occurrence of, these institutional data breaches, proper auditing, access-control, and chain-of-custody procedures need to be mandated and enforced.

Dealing with the technological ecosystem as a whole, any guideline issued by the Canadian government should also take a page from the joint guidelines of the Japanese Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry, and note explicitly the application of *PIPEDA* to NFC technology where personally-identifying information is collected, or where the technology's usage allows for inferences as to a person's identity. By issuing such guidelines, Industry Canada can make clear from the start that data collected through NFC devices deserves the same protections and respect as personally-identifying information collected from more traditional means such as loyalty cards or in-store surveys.

While emphasizing the applicability of *PIPEDA* to NFC technology, Industry Canada must also work with stakeholders to increase public awareness of the technology to spur on its wider adoption. As the METI Guidelines state, it is incumbent upon both industry stakeholders, and the government, to undertake public awareness campaigns to educate consumers on the nature and benefits of new technology. Such a guideline would find particular relevance in Canada, where the failure of Ontario's public sector smart-card system launch, and indeed, the entire project, was attributable, in part, to the failure of both industry and government to properly inform the public of the nature of the proposed smart-card system.[114]

---

110 US Department of State, "The US E-passport Frequently Asked questions" online: US Department of State <http://travel.state.gov/passport/passport_2788.html>.

111 Privacy by Design, *supra* note 37 at 208.

112 *Ibid.* at 280.

113 *Ibid.* at 280-281.

114 Stuart Bailey & Nadia Caidi, "How much is too little? Privacy and smart-cards in Hong Kong and Ontario" (2005) 31 J of Info Science 361.

By mandating the above proposals, the government can anticipate, and preempt, the identified weaknesses in NFC technology; namely, uncertainty as to its relationship with *PIPEDA* and general shortcomings in terms of properly securing personally-identifying information. This is preferable to a reactive wait-and-see approach, which would only act after a large, but preventable, data breach. As well, by acting early the government can foster a "culture of privacy"[115] among NFC stakeholders from the beginning, which ultimately benefits consumers.

(c) Power (and Teeth) to the Federal Privacy Commissioner

The issue of Canada's Privacy Commissioner must also be addressed. While not dealing with NFC-technology specifically, but rather with the broader privacy ecosystem in which it operates, a final recommendation would involve expanding the powers of Canada's Privacy Commissioner to include the ability to issue fines, compliance orders, and even promulgate industry guidelines, if necessary.

Commentators have long noted the lack of "teeth" vested in Canada's Privacy Commissioner and questioned the effectiveness of the ombudsman model.[116] The BC Civil Liberties Association, in its 2006 report, also calls for broadened powers for the Privacy Commissioner in terms of order-making and regulatory powers.[117] An interesting proposal contained within the BCCLA report also calls for the ability of the Privacy Commissioner to award damages to complainants, similar to the power enjoyed by Human Rights Tribunals in Canada, and by Privacy Commissioners in other jurisdictions.[118]

Relating to guideline-issuing powers, other jurisdictions have vested their Privacy Commissioners with such abilities. In New Zealand, for instance, the Privacy Commissioner works with industry to create best practice guidelines which, once adopted by the Commissioner, have the force of law within the country.[119] It is noted that by encouraging industry towards responsible internal self-regulation, Privacy Commissioners can better dedicate scarce resources elsewhere.[120] Vesting Canada's Privacy Commissioner with guideline-making powers may also allow for quicker action in relation to emerging technologies. Should Industry Canada guidelines be delayed through red-tape, the Privacy Commissioner may fill the gap with interim, but still binding, guidelines until the government can issue its definitive set of mandates to industry.

Such a recommendation for expanding the Privacy Commissioner's powers is not without controversy. Empowering the Privacy Commissioner with binding powers changes the essential role of the Commissioner. Rather than being an ombudsman, the Commissioner then becomes an "ombudsman with a stick", which

---

115 *Ibid.* at 302.

116 Privacy Watchdog, *supra* note 89.

117 BCCLA Report, *supra* note 92 at 85.

118 *Ibid.* at 87.

119 *Privacy Act 1993* (NZ), 1993/28, RS at s 53(a) and (b), online: Parliament Counsel Office <http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html> [NZ *Privacy Act*].

120 BCCLA Report, *supra* note 92 at 62.

in essence creates a more adversarial quasi-regulatory power similar to that of a Human Rights Tribunal as discussed above.[121] Such a change in framework has been resisted by even Privacy Commissioners themselves. Speaking at a CENTRUM Conference in Toronto, then-Privacy Commissioner Bruce Phillips stated "I have no powers of enforcement and . . . I want no powers of enforcement. Neither I, nor my staff, want these powers."[122] Jennifer Stoddart shared this view as recently as 2005, criticizing the "adversarial, litigious and less flexible approach" of regulatory models dealing with privacy violations.[123] One further notes that in its 5-year review of *PIPEDA*, the Standing Committee on Access to Information, Privacy and Ethics also rejected the idea of granting broader powers to the Privacy Commissioner.[124]

The above objections aside, however, the ombudsman model's time in the sun has passed. While Canada's Privacy Commissioner has scored notable, and surprising, victories against tech giants Facebook and Google, compliance among small-to-medium sized businesses is noticeably lacking.[125] A recent CBC investigation, for example, revealed poor compliance with notice requirements for businesses making use of closed-circuit surveillance systems.[126] This has particular relevance to NFC technology, as business operators' compliance in regard to informed consent is especially important in an NFC context given the invisible nature of the data collection that occurs. Commentators note that perhaps the best way to get the attention of small- and medium-sized privacy violators, who currently have little, if any, incentive to cooperate with the Privacy Commissioner is through the imposition of fines.[127]

Looking overseas, a number of jurisdictions employing an ombudsman model in regard to privacy protection are transitioning to a regulatory framework that al-

---

121 Department of Justice, "The offices of the information and privacy commissioners: The merger and related issues" (3 August 2012), online: Department of Justice <http://www.justice.gc.ca/eng/ip/p7.html>.

122 Bruce Phillips, Speaking notes prepared for the CENTRUM Conference: "The Privacy Commissioner of Canada's approach to implementing the Act" (10 December 1999), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/sp-d/archive/02_05_a_991210_e.asp>.

123 Jennifer Stoddard, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model Under *PIPEDA*" (October 2005), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/research-recherche/2005/omb_051021_e.asp>.

124 House of Comons, Standing Committee on Access to Information, Privacy and Ethics, *Statutory Review of the Personal Information Protection and Electronic Documents Act Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, (Chair: Tom Wappel) (May 2007) at 34, online: Parliament of Canada <http://www.parl.gc.ca/content/hoc/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-e.pdf>.

125 BCCLA Report, *supra* note 92 at 42.

126 Maureen Brosnahan, "Store video cameras failing to comply with privacy laws" *CBC News* (28 December 2012), online: CBC News <http://www.cbc.ca/news/canada/story/2012/12/27/video-surveillance-cameras.html>.

127 BCCLA Report, *supra* note 92 at 85.

lows their Privacy Commissioners greater powers, including the ability to levy fines.[128] Increasingly, Canada stands alone in its embrace of the ombudsman model in relation to privacy protection. Perhaps most telling, Jennifer Stoddart, reversing her position from 2005, also now calls for greater powers for her office, including fining authority, commenting that respondents "pay lip service to our concerns and then ignore our advice."[129]

Rapid advances in technology, not just in relation to NFC, bring with them new and more complex privacy challenges. Canada's Privacy Commissioner must be able to address those privacy concerns through coercive means if necessary. The case of NFC is a prime example; with the technology's ability to rapidly build profiles on individual users, it is imperative that the Privacy Commissioner be able to compel compliance with *PIPEDA* to undercut potential leaks or misuse of personal information gleaned through NFC usage.

V. CONCLUSION

Near-field Communication technology brings with it both benefits and challenges. When utilized properly, NFC-enabled devices serve as an effective cash replacement, allowing for rapid, convenient micro-payments in a number of commercial and commuting settings. It is, however, also a technology which carries its own set of privacy-related challenges. NFC-enabled devices leave a long electronic trail, allowing for building profiles of individual consumers with relative ease. Moreover, large amounts of personally-identifying information are also gathered, and stored on, the NFC-devices themselves, as well as the databases under which NFC technology operates.

As noted above, some countries, such as Japan, took a pro-active approach to NFC technology. Clear industry guidelines were promulgated by various ministries of the Japanese government, and the Japanese *Penal Code* contains broad language that captures NFC-technology in its various anti-fraud provisions. Canada, by comparison, lags in dealing with NFC technology. This can be partially excused given that the technology is still in its infancy in Canada; however, it is a technology poised for widespread adoption in the country. Given that, it is imperative that Canada position itself to proactively deal with the privacy challenges raised by NFC technology. In that regard, clear, binding guidelines, either from Industry Canada or Canada's Privacy Commissioner, are necessary to make clear the applicability of *PIPEDA* to the technology, and for setting out best-practices for securing users' personally-identifying information. An amendment to Canada's *Criminal Code*

---

128 France Houle & Lorne Sossin, "Powers and Functions of the Ombudsman in the *Personal Information Protection and Electronic Documents Act*: An Effectiveness Study" Office of the Privacy Commissioner of Canada (August 2010) at 126, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/research-recherche/2010/pipeda_h_s_e.pdf> [Houle and Sossin].

129 Inayat Singh, "Stoddart calls for sharper teeth, power to levy fines to better protect privacy" *CTV News* (11 December 2012), online: CTV News <http://winnipeg.ctvnews.ca/stoddart-calls-for-sharper-teeth-power-to-levy-fines-to-better-protect-privacy-1.1075652>.

dealing with the maladministration of NFC devices and cards would also be of benefit, and eliminate any uncertainty in the law.

Perhaps the biggest aid in the smooth adoption of NFC technology on a widespread basis, and to privacy protection in general, is expanding the powers currently enjoyed by Canada's Privacy Commissioner. Such expanded powers are not unheard of in the Commonwealth, as noted above, and even in Canada at a provincial level; Alberta and British Columbia utilize a "hybrid" model which allows limited sanctioning powers to its Privacy Commissioners.[130] Moving away from an ombudsman approach, the Privacy Commissioner can compel greater compliance through stronger enforcement powers, particularly among small to medium-sized businesses.

It is clear that Canada must adjust its approach to deal with the future widespread adoption of NFC technology in the country. This is not an insurmountable task; Canada does have a privacy and regulatory framework in place and thus the answer rests in tweaking that system, rather than in building it from the ground up. In that regard, amending the *Criminal Code*, creating clear industry guidelines, and redefining the role of the Privacy Commissioner are all means by which Canada can pre-empt, and eventually benefit from, the widespread use of NFC technology.

130 Houle & Sossin, *supra* note 128 at 167.