

Cross Border Identity Management Background Paper

This background paper addresses some of the card technology industry's concerns about the use of vicinity or long range (read) RFID for identity management.

Many of these concerns come from companies that produce RF technology, but feel that this technology does not have the privacy enabling attributes required for identity management.

We are submitting this information in the event that the Government of Canada chooses to consider the same technology and practices being proposed by the United States government. Given the shared border, there is a high degree of likelihood that this is the case in order to pursue efficiencies of sharing infrastructure and/or citizen information.

In this paper, I have addressed specific fair information practices in terms of identifying known areas of concern, as well as areas where information has not been made available.

RFID Technology

Let me start with the technology. The current proposal for cross border identification is a radio frequency tag technology capable of transmitting information at ranges exceeding 30 feet. It does not have the capability of blocking unauthorized readers.

The privacy risk is that tag information can be read without the citizen being aware, and can be read by readers normally employed for ID in hotels, retail outlets such as Wal-Mart's where it is used for inventory control and in companies where employees use it for physical and logical access control.

The mitigation argument is that citizens can keep their tag in a shielded envelope, but there is no guarantee that this will then fit into a wallet. At a minimum, the sole responsibility for ensuring the appropriate reading of information from the tag will fall to the citizen.

The second argument is that only a file number is on the tag, but that number identifies the citizen's record on a database. There is no evidence that adequate privacy protection or security has been designed for the overall system, including the networked data.

Another significant risk comes from the ease with which this technology can be cloned and copied. This is reminiscent of the cell phone cloning that took place in the early days of deployment in North America.

If this is done with identity, someone with a reader could capture the record number of a legitimate citizen with a similar physical appearance; they could then travel as that person. If the legitimate citizen is subsequently detained because of actions taken by the imposter, we question whether the rights of fair information practices would be granted.

Cross Border Identity Management Background Paper

This technology, used for cross border identity management could enable identity theft and personal tracking.

Accountability

If these tags can be read by readers other than government controlled, who is accountable? The argument will be made that the information on the tag is not personal, so accountability does not apply. Given that the tag information leads to significant personal information, accountability should apply.

Recognition and Respect for Privacy

Given that tags are proposed to be optional, our only concern is that citizens understand the privacy implications.

Openness

We have not yet seen how this would be handled through policies and procedures.

Purpose Specification

We have been advised that federal border officers will have access to Washington State citizen records during a trial, but it is unclear how secondary data usage will be authorized and controlled. This is true for the trial and a national rollout. It is unlikely that national cross border identification could have been specified for collection of state related information.

Collection Limitations

Any use by federal agencies of existing state or provincial data would not have been collected directly from citizens, although this could be done moving forward. Direct access to state or provincial citizen databases should not be available.

Notification and Use

For both of these there is no evidence that state citizens were notified during the Washington trial, so clear policies and procedures would be needed in the event of a Canadian decision to adopt a similar program. In the event vicinity RFID is used, the ability to do this would be impossible, given that all RFID readers, used by both public and private entities would be reading data from the citizen's tag.

Right of Access / Right of Correction / Accuracy / Retention and Disposal

As with notification and use, the ability of all RFID readers to read the tag data, makes this virtually impossible. Concerns are also raised by the difficulty to access and/or correct personal data from no-fly lists.

Disclosure and Security

The back end systems components also raise concerns. There will be a large aggregation of personal information records on a database (or series of databases), increasing their value as targets. This is further complicated by data copied from the database to workstations at border points, raising concerns of unintentional release or

Cross Border Identity Management Background Paper

sharing of personal data. It is not clear how or when information will be cleared from workstations after use.

Government data breaches in both Canada and the United States serve as a warning that more security is required, not just to stop external threats, but also to clearly define what employees and contractors are allowed to do with data, and effectively enforce those rules.

Aggregation

The issue here is compounded when tag data is read by non-border crossing entities. For example, a commercial store reads the tag, has payment data also available from the purchase made in the store and has a list of items or services bought. They may then choose to ask the customer for their name and other personal information. The customer is unaware that every time they enter the store from that point on, the store will be aware if the customer has the tag in their wallet.

Anonymity and Pseudonymity

At the very least, there is an ability to know where a specific tag holder is or has been. Linking the identity of the tag number to the individual can be accomplished through a number of methods.

Recommendations

1. Privacy Impact Assessment

A systemic privacy impact assessment is a fundamental requirement at this point. We would like to see it conducted by an independent third party. The Contactless Smart Card Applications Design Tool And Privacy Impact Assessment from ACT Canada is available at www.actcda.com or from and the office of the Information and Privacy Commissioner Ontario at www.ipc.on.ca.

This request has been made of the appropriate US government departments. If Canadian governments, at either the federal or provincial levels are considering any changes to cross border ID, we would recommend that they also undertake this assessment.

2. Technology Choices

The contactless nature of RFID has advantages, but lacks sufficient security for identity management. The following outlines other contactless technologies that provide privacy enabling applications, as well as a comparison between contactless and RFID technology.

Contactless Technology vs. Radio Frequency Identification (RFID)

A contactless card is a smart card that uses radio frequencies to communicate with compatible terminals (readers) through the antenna embedded into the card. This

Cross Border Identity Management Background Paper

differs from a contact card that is inserted into a reader so that data can be communicated. Contactless cards contain microprocessor chips that support various security tools, including encryption, to protect data as it is transmitted between the card and the reader. International standards allow contactless cards to operate at limited distances from less than a millimetre to 10 centimetres. For this reason, these are often referred to as proximity cards.

RFID tags are simple, low-cost and disposable electronic devices that are currently used to identify animals, track goods through a supply chain or to replace printed bar codes at retailers. RFID tags include an integrated circuit that typically stores a static number (an ID) and an antenna that enables the chip to transmit the stored number to a reader. When the tag comes within range of the appropriate RF reader, the tag is powered by the reader's RF field and transmits its ID to the reader. There is little to no security on the RFID tag or during communication with the reader, although the data on the chip may be encrypted. Typical RFID tags can be easily read from distances of several centimetres to several metres to allow easy tracking of goods. They are sometimes referred to as vicinity (read) cards or tags.

Switch Cards

New technology entering the marketplace incorporates an on/off switch built into the card. When a customer wishes to allow someone to read data from the card they press the switch. This allows the customer to control when data is available. The application owner should design their application to ensure that systems, while working with individual level data instead of in the supply chain or similar areas, are privacy-enabled end-to-end. This specifically means informing and engaging individuals so that they are making informed choices.

Contactless cards with an on/off switch allow consumers to control when their card information is accessed. Unless they press and hold the switch, which is built into the card itself, no one can access any applications or data on the card. This is true of all contactless switch cards, regardless of whether they use proximity or long-range read technology. It is important to note that not all contactless cards have switches. Also, the same privacy protection and security measures you choose for a non-switch card should be implemented on a switch card, for those times when the switch card is in an 'on' mode.

We would call for the use of contactless, not RFID, technology to support any government identity management applications.