Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practice: Consultation Paper

Office of the Privacy Commissioner of Canada

SUBMISSIONS OF
THE AMALGAMATED TRANSIT UNION, CANADIAN COUNCIL

Amalgamated Transit Union, Canadian Council
61 International Blvd.
Suite 210
Rexdale, ON
M9W 6K4
T: (416) 679-8846
F: (416) 679-9195

Robin G. West
Canadian Director

TABLE OF CONTENTS

INTRODUCTION

These are the submissions of the Amalgamated Transit Union ("ATU") Canadian Council in response to the Office of the Privacy Commissioner of Canada's request for submissions on the consultation paper entitled "Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices."

The ATU Canadian Council commends the Privacy Commissioner for taking a proactive approach to the development of best practices for the use of RFID technology in the workplace.

As recognised by the Privacy Commissioner, "what happens in the workplace – including how the workplace responds to matters such as privacy – can have a profound effect on employees' sense of dignity, their sense of freedom, their sense of autonomy."[1] As discussed herein, the ATU Canadian Council takes the position that individual privacy is of paramount importance and RFID technology must not be used to subvert that right.

The Amalgamated Transit Union & The Canadian Council

Founded in 1892, at present the ATU is the largest labour union for transit workers in North America. Today the union has over 180,000 members in over 273 local unions in 46 states and 9 provinces. The ATU membership includes bus, subway, light rail and ferry operators, clerks, baggage handlers, mechanics and others in public transit, inter-city and school bus industries.

Established in 1982, the Canadian Council is the highest authority and voice in Canada for the ATU on all issues of Canadian interest including legislation, political, educational, health and safety, cultural and social welfare matters.

SUBMISSIONS

1. Where RFID systems are used in a workplace, human dignity needs to be considered and the 4-part reasonable person test should guide their use.

a. What uses of RFID systems should be forbidden in the workplace?

i. Covert Surveillance

The ATU Canadian Council takes the position that the covert use of RFID technology should be forbidden.

RFID technology must not be used in the workplace to monitor and track employee movements. When used in combination with Global Positioning System technology, it is possible that a tag, linked to other information, is capable of identifying an individual and as such, the individual's movements become capable of being tracked in real time and space.[2] As stated in the Consultation Paper, it has been recognized that "continuous, indiscriminate surveillance of employees … [is] based on a lack of trust … The effect … of such omnipresent observation was stifling."[3] Constant surveillance and observation has a detrimental effect on employee morale and trust and can often cause an increase in stress. Indiscriminate surveillance of employees is dehumanizing and the ATU Canadian Council is strongly opposed to the use of RFID technology for this purpose.

ii. The Use of RFID Generated Information for Disciplinary Purposes

Information generated from RFID data collection, such as entry/exit times, location, or time spent in a particular area/task must never be used for the purposes of employee discipline.

As discussed below, the data generated from an RFID tag must remain anonymous and should not be linked to any company data such as personnel or medical records which would identify the individual.

iii. The Use of RFID Technology to Undermine the Right to Collective Representation

The right to freedom of association is the cornerstone of modern labour relations.[4] The Supreme Court of Canada has acknowledged and affirmed such, recognising that because "workers have the right to bargain collectively as part of their freedom to associate [it] reaffirms the values of dignity, personal autonomy, equality and democracy that are inherent in the *Charter*."[5] This right to collective

representation is enshrined in both provincial and federal labour legislation and is further protected under the *Canadian Charter of Rights and Freedoms*.

RFID technology must not be used in such a way as to interfere with or subvert the right of workers to seek collective representation.[6] Any such use of RFID technology is illegal and therefore must be forbidden.

If employers are able to track employee movement, it makes it more difficult for those workers to coordinate membership drives and organizing activities. Furthermore, RFID technology must not be used to undermine the ability of unions to represent their members.

The ATU Canadian Council supports the rights of workers to collective representation and RFID technology should not be employed to undermine such.

b. What should the parameters be?

While the most common use of RFID tags in the workplace is in staff passes and identity badges worn to control entry into buildings and rooms, the variety of RFID applications is endless given the minute size of most RFID tags. These tags can be sewn into employee uniforms, attached to tools or equipment and even be implanted into an employee's skin.

i. The Use of RFID Technology Must Be Justified on an Objective Standard

The ATU Canadian Council takes the position that prior to the introduction of any such technology into the workplace, the onus is on the employer to justify on an objective standard that the use of RFID technology is based on a purported legitimate business purpose.

Any efforts to seek to introduce RFID into workplace for purported legitimate business purposes must be balanced against the right to privacy. As such, it is necessary for the employer, in consultation with the Union, to develop policies and practices to ensure that this technology is not used to monitor employees or for any improper purpose.

ii. The Union as Exclusive Bargaining Agent

Within a unionized workplace, the Union is the exclusive bargaining agent for all those employees it represents. This right of representation is statutorily recognized in provincial labour legislation across Canada and at the federal level under the *Canada Labour Code*. As such, the Union routinely negotiates the terms and conditions of employment for its members with the employer. Given this exclusive bargaining relationship, an employer must seek the consent of the Union prior to the introduction of RFID technology.

Aside from establishing that the use of RFID technology is based on a legitimate business objective, the ability of an employer to introduce such will be constrained by the terms of the collective agreement between the parties. Given that this new technology may or may not be contemplated within the collective agreement, it is incumbent upon the employer to negotiate its use with the Union and to come up with a mutually agreeable protocol for such.

iii. The Requirement of Union Consent

The ATU Canadian Council agrees with the Commissioner's position that employees and unions should be consulted by employers prior to the introduction of any workplace surveillance system, including RFID technology. As discussed above, it is our position that it is incumbent upon the employer to seek the consent of the Union to introduce such technology, given the role of the Union as the exclusive bargaining agent.

Any introduction of such technology in the workplace must be linked to an explicit commitment from the employer that it will maintain the individual dignity and privacy rights of its employees.

iv. Minimum Requirements for an RFID Workplace Policy

Prior to the introduction or use of RFID technology in the workplace, the employer should be required to provide its employees with a clear and simple explanation of how RFID works. At a minimum, this explanation should include details about where RFID tags are located, what types of RFID tags are used and their geographical scope.[7]

Further, any employer using RFID should be required to have a written policy governing its use. Such a policy must be negotiated with the Union. The policy should set out:

a) the nature of the data being collected;

b) the purpose for which the data is being collected

c) an explicit commitment that the data collected will not be linked to any other personal information, including but not limited to personnel and medical records

d) access and retention policies;

e) procedures for dealing with unauthorized use of the data;

f) the consequences of such unauthorized use;

g) the terms and conditions of third party access (if any); and

h) how the implementation and application of the RFID policy is monitored and consequences for its breach.[8]

v. Fair Information Principles

Any use of RFID technologies must be done in compliance with the principles of the Fair Information Principles contained in Schedule 1 of *PIPEDA*. The above listed policy requirements will be discussed in light of these Principles.

a. Principle 1 – Accountability

If RFID technology is introduced, the employer is responsible for personal information under its control and must be accountable for its compliance with the provisions of *PIPEDA* and the terms of the negotiated RFID policy.

No individual with direct supervisory control over an employee or from Human Resources should be in charge of any data generated by RFID technology. As discussed above, such data should not be associated or linked with any personal information and must remain anonymous.

b. Principle 2 – Identifying Purposes

Principle 2 states that "the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected." If RFID technology is introduced into the workplace, the use of the data collected must be restricted to the purpose for which it was originally intended.

For example, if staff access passes are RFID enabled for the purposes of allowing individual employees access to different parts of the workplace, the data collected from the RFID tags must only be used for this purpose. If the employer seeks to use this data for other purposes, such as time keeping, the employer should not be permitted to do so, absent negotiation and agreement from the Union.[9]

Furthermore, the data collected from RFID technologies should not be used for performance assessment or disciplinary purposes. Employees should also have the right to switch off RFID tags or to remove them when taking breaks or after-hours without penalty.

c. Principle 3 – Consent

Principle 3 states that "knowledge and consent of the individual are required for the collection, use or disclosure of personal information." As discussed above, as

the Union is the exclusive bargaining agent for its members, consent of the Union must be obtained prior to the introduction, use or disclosure of any RFID technologies in the workplace. The ATU Canadian Council takes the position that it is inappropriate for an employer to use RFID generated data for covert employee surveillance or any other improper purpose.

Any consent should be informed and as such, the employer must be required to explain the technology and its purported use. As discussed above, the employer must also establish that the introduction of such is based on a purported legitimate business objective.

d. Principle 4 – Limiting Collection

The collection of information generated by RFID tags must be limited to the purpose for which the technology was introduced. This information must be collected by fair and lawful means. The ATU Canadian Council takes the position that employee surveillance and monitoring is not a legitimate purpose and therefore any RFID information cannot be used for such. RFID generated data must not be collected indiscriminately and an employer must explicitly outline the type and amount of information that is being collected.

e. Principle 5 – Limiting Use, Disclosure and Retention.

Information collected by RFID technology cannot be used or disclosed for purposes other than those for which it was collected. Such information must only be retained as long as necessary for the fulfillment of those purposes. As stated above, any RFID generated information cannot be used for disciplinary, surveillance or time keeping purposes.

Any RFID information that is no longer required to fulfill the identified purposes should be destroyed and erased. Prior to the introduction of any RFID technology, the employer, in negotiation with the Union, must develop clear guidelines as to the length of time such data will be retained and policies with respect to the destruction of such information.

f. Principle 6 - Accuracy

Any personal information collected must be accurate and complete. While the ATU Canadian Council takes the position that any RFID generated data must remain anonymous and must not be linked to any other personal information, all employees should have access to any information collected and have the opportunity to correct any mistakes in the data collected. [10]

Again, the ATU Canadian Council strongly states that no RFID data must ever be used for disciplinary or other improper purposes.

g. Principle 7 – Safeguards

Any information generated from RFID tags must be protected and there cannot be any unauthorized use of the data collected. In conjunction with the Union, the employer must outline procedures and consequences for the unauthorized use of data collected. The ATU Canadian Council takes the position that the employer must negotiate with the Union to develop and implement rigid controls to ensure that there is no unauthorized use of RFID technology or any RFID generated data.

Furthermore, any data collected by the employer should not be sold or given to any third party. This concern is particularly pressing in light of the *USA PATRIOT Act*, as discussed below.

h. Principle 8 – Openness

All RFID policies must be negotiated with the Union and be made available to all employees. The employer should post copies of the policy within the workplace in a location accessible to all employees.

i. Principle 9 – Individual Access

As discussed under Principle 6, all employees must have access to any information collected and have the opportunity to correct any mistakes in the data. The affected employee and the Union must be informed of the existence, use and disclosure of any information and shall be given access to such information. Any employee must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Again, the ATU Canadian Council reiterates its position that any RFID generated data must remain anonymous and must not be linked to any other personal information or be used for any improper purpose.

j. Principle 10 – Challenging Compliance

The Union has the right to raise a challenge concerning the employer's compliance or non-compliance with the negotiated RFID policies. The Union has the right to raise such under *PIPEDA*, the collective agreement and through any other legal means.

2. Employers should consult employees (and unions) before the introduction of workplace surveillance systems or technologies with surveillance capabilities, such as RFID.

As noted above, the ATU Canadian Council takes the position that the covert use of RFID technology should be forbidden. The onus is on the employer to demonstrate on an objective standard that the purpose for which RFID technology is introduced is a legitimate business objective. The use of any RFID technologies in the workplace is subject to negotiations with and the consent of the Union.

a. Do you believe any particular group or type of workers may be particularly disadvantaged as a result of surveillance by RFID systems?

As the representative of thousands of transit workers across Canada, one of the ATU Canadian Council's primary concerns is the impact of RFID technology on transit. If RFID systems are introduced, for example, to monitor routes etc., by correlation, the bus operator is inevitably being monitored. Steps must be taken to ensure that personal information, such as which route or bus is being driven by which operator is not linked to the information generated from the RFID tag on the bus in issue.

Furthermore, as discussed above, the ATU Canadian Council is concerned about the possibilities that RFID technology could be used by employers to interfere with union organizing or collective bargaining.

3. Employees must be told whether RFID-related information will be linked with other personal information and whether the information will be available to third parties.

a. What linkages should be forbidden?

As discussed above, the onus is on the employer to demonstrate on an objective standard that the purpose for which RFID technology is introduced is a legitimate business objective. Any information collected must be strictly confined to the purported business objective and must be anonymous.

The ATU Canadian Council takes the position that RFID related information should not be linked to any other personal information possessed by the employer, such as medical records, personnel files or disciplinary history. Such linkages would permit the employer to identify the individual associated with a particular RFID tag and therefore raise the prospect of monitoring individual employees and utilizing RFID related information for disciplinary or other improper purposes.

b. What personal information from elsewhere in the organization might it be reasonable to link to an RFID and under what circumstances?

Again, as stated above, the ATU Canadian Council takes the position that no personal information should be linked to an individual RFID tag.

4. Implanting employees with RFID tags against their will is unacceptable under any circumstances. Employment should never be made contingent on a willingness to be implanted with an RFID tag.

a. What other considerations need to be brought to bear on the discussion of RFID implants in the workplace?

The ATU Canadian Council agrees with the Commissioner's position that no employee should ever be required to implant an RFID tag, or any device, into their person as a condition of employment. Requiring an employee to do so is a fundamental violation of personal autonomy and dignity.

i. Lack of Off Duty Privacy

The use of implanted RFID tags raises a number of concerns. Firstly, individuals with implanted RFID tags would never be "off duty" as their activities could be monitored around the clock, including the employee's conduct after work, during lunch and even during bathroom breaks. If the RFID generated data is combined with other technologies like GPS systems, an employee may be monitored at all times, including after hours and on vacation. This is an unacceptable intrusion into an employee's right to privacy.

ii. Third Party Access

Further, if an employee is capable of being tracked at all times, the issue of third party access to the information generated by the RFID implant arises. For example, would an insurance company, the government or other authorities be able to use the RFID implant to track the movements of the employee in question for use in an investigation?

iii. Security

Security is another major concern associated with the use of implanted RFID tags - if the RFID implant is used to allow the employee access to sensitive or secure areas, the presence of such an implant may pose a legitimate safety and security threat to the employee in question.

iv. Health Concerns

Furthermore, there is no comprehensive data on the long term health effects of such implants. At least one study has concluded that chip implants "induced" malignant tumours in some lab mice and rats.[11] Although approved by the US Food and Drug Administration for medical use, it noted a number of risks associated with implanted RFID tags, including the possibility that the subcutaneous tag could interfere with defibrillators, the tags may be incompatible with MRI scans and the potential for the tags to migrate around the body thereby making them difficult to extract. [12]

Given the invasive level of this technology, it is difficult to imagine any legitimate employer need or interest which would outweigh the gross invasion of an employee's privacy.

v. Legislation Banning Forced Implants

A number of American states have passed legislation making it a crime to require an individual to be implanted with RFID technology. In May 2006, Bill 290 unanimously passed in both houses of the Wisconsin state legislature, making it illegal to require an individual to be implanted with a microchip. Any person who violates the law will be fined up to $10,000 each day it is in contravention of the Act.[13] North Dakota passed similar legislation in April 2007.[14] Legislation was also passed in California in 2007 not only making it illegal to force someone to be implanted but also creating a civil right of action against the violator.[15] The ATU Canadian Council recommends that the Privacy Commissioner recommend and support similar legislation in Canada.

In light of the above, the ATU Canadian Council takes the position that no employee should ever be required to implant an RFID device as a condition of employment.

5. What strategies would you recommend for the community of privacy commissioners to best deal with this issue in the years ahead?

Individual autonomy and privacy is a right which should be valued and protected, particularly in light of new monitoring technologies. As such, the ATU Canadian Council commends the Privacy Commissioner for engaging in the present consultation and encourages the Commissioner to continue to do so with respect to this issue in the future.

The participation of employees, employers and unions in developing "best practices" with respect to RFID technology is essential as it is those parties who will be primarily affected by the use of RFID in the workplace. As the Union is the exclusive bargaining agent of its members, the introduction of any such technology is subject to negotiations with and the consent of the Union.

As the use of RFID technology in the workplace is likely to grow in the upcoming years, the ATU Canadian Council urges the Commissioner to ensure that its policies with respect to this issue are revised in accordance with new developments. The ATU Canadian Council also encourages the Commissioner to continue to educate both employers and employees about the uses of RFID technology and the impact of such on individual privacy rights.

AREAS OF CONCERN

1. The *USA PATRIOT Act*

The *Act* permits American law enforcement officials to seek a court order that allows access to the personal records of any person without that person's knowledge. As such, U.S. officials could access information about Canadians if that information is physically within the United States or accessible electronically.[16]

For example, if a Canadian company out-sources their data processing to the United States, stores their information at a US branch of the same company or shares and/or sells information to a US based company, that information will be subject to the provisions of the *USA PATRIOT Act.*

The *Act* also permits US authorities to gain access to the personal information of Canadians even if the information is not held within the United States. For example, if data is outsourced to a US linked company based in Canada, it is possible that US authorities may assert jurisdiction over the company and thus the information, even though it is physically located in Canada.[17] Arguably, any information held by a US based company is subject to the terms of the *PATRIOT Act*.

Given the extensive powers of American officials under the *PATRIOT Act*, the ATU Canadian Council is very concerned about the security of any data, personal or otherwise, generated by RFID tags. As such, the ATU Canadian Council again strongly stresses that any information collected from RFID technology must not be linked with any employee information which would allow the individual's behaviour to be monitored or activities tracked.

Furthermore, access under the *PATRIOT Act* subverts the rights of employees under *PIPEDA* and eradicates all protections provided therein.

In light of the above, employers should be precluded from using RFID technology if it is accessible under the *PATRIOT Act*.

2. Consequences of Breach

The ATU Canadian Council believes that it is critical that the privacy rights of Canadians and its members are protected. As such, strong enforcement mechanisms are required. In tandem to effective protection, effective consequences are required to prevent a breach before one occurs.

While there are statutory remedies under PIPEDA, these remedies must be consistently enforced. No employer should be able to violate the privacy rights of its employees without suffering serious consequences. Furthermore, no employee should ever face a reprisal as a result of his/her efforts to assert his/her statutory rights.

CONCLUSION

As discussed above, given the invasive nature of RFID technology, the ATU Canadian Council takes the position that the introduction of such must be justified by the employer and cannot be used in the workplace without the consent of the Union.

If RFID technology is introduced in the workplace, the terms of its use must be negotiated with the Union and any use must be in accordance with Fair Information Principles. As such, the covert use of RFID technology should be forbidden. Furthermore, RFID generated information must remain anonymous and should not be linked with any other personal information or used for disciplinary purposes.

ENDNOTES

[1] - Jennifer Stoddart, "Privacy in the Workplace", *Office of the Privacy Commissioner of Canada*, April 11, 2006, http://www.privcom.gc.ca/speech/2006/sp-d_060411_e.asp (Accessed April 16, 2008)
[2] - "Fact Sheet: RFID Technology," *Office of the Privacy Commissioner of Canada*, n.d., http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp (Accessed April 7, 2008)
[3] - "Radio Frequency Identification (RFID) in the Workplace: Recommendations and Good Practices", *Office of the Privacy Commissioner of* Canada, March 2008, at p. 17.
[4] - *Health Services and Support – Facilities Subsector Bargaining Assn. v. British Columbia,* [2007] S.C.J. No. 27 at para 84.
[5] - *Health Services and Support – Facilities Subsector Bargaining Assn. v. British Columbia,* [2007] S.C.J. No. 27 at para 86.
[6] - "RFID in the Workplace: UNI Code of Good Practice," *Union Network International*, April 27, 2006 http://www.union-network.org/uniindep.nsf/2702f48e48fad7dac125718e0034fd79/$FILE/RFIDdraft.pdf (April 8, 2008)
[7] - "RFID in the Workplace: UNI Code of Good Practice," *Union Network International*, April 27, 2006 http://www.union-network.org/uniindep.nsf/2702f48e48fad7dac125718e0034fd79/$FILE/RFIDdraft.pdf (April 8, 2008)
[8] - "RFID in the Workplace: UNI Code of Good Practice," *Union Network International*, April 27, 2006 http://www.union-network.org/uniindep.nsf/2702f48e48fad7dac125718e0034fd79/$FILE/RFIDdraft.pdf (April 8, 2008)
[9] - "RFID in the Workplace: UNI Code of Good Practice," *Union Network International*, April 27, 2006 http://www.union-network.org/uniindep.nsf/2702f48e48fad7dac125718e0034fd79/$FILE/RFIDdraft.pdf (April 8, 2008)
[10] - "RFID in the Workplace: UNI Code of Good Practice," *Union Network International*, April 27, 2006 http://www.union-network.org/uniindep.nsf/2702f48e48fad7dac125718e0034fd79/$FILE/RFIDdraft.pdf (April 8, 2008)
[11] - Todd Lewan, "Chip Implants Linked to Animal Tumors," *Associated Press*, September 8, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html (April 8, 2008)
[12] - Todd Lewan, "Chip Implants Linked to Animal Tumors," *Associated Press*, September 8, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html (April 8, 2008)
[13] - "Wisconsin Bans Forced Human RFID Chipping", *SpyChips.com*, May 31, 2006, http://www.spychips.com/press-releases/verichip-wisconsin-ban.html (Accessed April 4, 2008)
[14] Marc L. Songini, "N.D. bans forced RFID Chipping," *Computerworld*, April 12, 2007

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&articleId=9016385 (Accessed April 10, 2008)

[15] Senate Bill 362, California, http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0351-0400/sb_362_bill_20070627_amended_asm_v95.pdf, (Accessed April 17, 2008)

[16] "Frequently Asked Questions: USA PATRIOT ACT," *Treasury Board of Canada Secretariat*, n.d., http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/usapa/faq_e.asp, (Accessed April 14, 2008)

[17] Patricia Kosseim, "Protecting Personal Information in Canada and Abroad," *Office of the Privacy Commissioner of Canada*, March 6, 2006, http://www.privcom.gc.ca/speech/2006/sp-d_060306_pk_e.asp, (Accessed April 16, 2008)