

## Burroughs, Sabrina

---

**From:** Levin, Toby  
**Sent:** Tuesday, August 22, 2006 5:44 PM  
**To:** PrivacyHQ  
**Subject:** IG RFID redacted report link

[http://www.dhs.gov/interweb/assetlibrary/OIGr\\_06-53\\_Jul06.pdf](http://www.dhs.gov/interweb/assetlibrary/OIGr_06-53_Jul06.pdf)

reported in

[http://www.washingtontechnology.com/news/1\\_1/daily\\_news/29176-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/29176-1.html)

Toby Milgrom Levin  
Senior Advisor  
The Privacy Office  
Department of Homeland Security  
Washington, DC 20528  
*Direct: 571.227.4128*  
*Privacy Office: 571.227.3813*  
*Fax: 571.227.4171*

(b)(2), (b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

## Burroughs, Sabrina

---

**From:** Sand, Peter  
**Sent:** Wednesday, November 02, 2005 8:49 AM  
**To:** Privacy Office  
**Subject:** FYI NEWS: RFID pioneering "privacy principles"

HID, Indala parent company ASSA ABLOY ITG releases pioneering “privacy principles”

Tuesday, November 1 2005

<http://www.contactlessnews.com/library/2005/11/01/hid-indala-parent-company-assa-abloy-itg-releases-pioneering-privacy-principles/>

One of the leading suppliers of security technology, ASSA ABLOY Identification Technology Group (ITG) has taken a proactive step to protect the privacy of a worldwide community of RFID end users. In September the company published its “corporate principles and practices” regarding RFID and privacy.

Assa Abloy ITG includes HID, Indala, OMNIKEY, Sokymat, Access ID, ACG, Synercard, Buga, and other leading organizations. President of HID and co-CEO of ITG, Denis Heber, said “we recognize that as our technology and the uses for it grow, the issue of privacy protection will become increasingly important for our customers and society at large.”

President of Indala, Marc Freundlich, suggested that the principles might extend beyond the ITG companies calling them, “substantial and meaningful steps we hope will become the industry standard.”

The following is a copy of the ITG Privacy Principles (numbers were added to aid in the reading of the document):

ITG supports the following business principles and practices in respect to its Radio Frequency Identification (RFID) products and services, in all cases consistent with applicable laws. ITG encourages buyers of our products and services to support the following fair information practices:

1. We support industry best practices through self-regulation, certifications, and other methods for protecting the security of personally identifiable information and other private data, and we believe that these practices should be auditable and enforceable.
2. We support the implementation of security for personally identifiable user information with protection that is proportional to threats to that data.
3. We recommend that any personal data stored on our products be subject to review by the user upon request. Personally identifiable information associated with a unique identifier on our products should be subject to reasonable fair information practices.
4. We do not intend for our products to be used for sharing any personally identifiable information, whether collected on or linked to the tag with other parties, unless there is the clear consent of the user.
5. We consider responsible use of our products to include only the collection of necessary personally identifiable information.
6. We do not support the use of ITG products or services for the purpose of tracking any person without their knowledge and consent.
7. We recommend that people be made aware of and consent to the use of an RFID tag on any product or personal effect, its purpose and use, including any data stored on that tag or any change in the intended purpose or use.
8. Finally, ITG will provide upon request consumer education for users to make informed, intelligent decisions about the use

of our products.

**Burroughs, Sabrina**

---

**From:** Levin, Toby  
**Sent:** Monday, May 01, 2006 9:50 AM  
**To:** Mortensen, Kenneth; Sand, Peter; Richards, Rebecca; Kropf, John  
**Subject:** BNA RFID Resources Compilation

Volume 5 Number 18  
 May 1, 2006  
 ISSN 1538-3431

Page 648

## Web Watch

### RFID

---

### RFID

### RFID

Web Watch is a periodic review of online resources prepared by the BNA Library's Laura Gordon-Murnane. For more information on government, industry, and academic links to a variety of timely topics, visit BNA's Web Watch online at <http://www.bna.com/webwatch>.

## UNITED STATES

### Commerce Department

*Radio Frequency Identification: Opportunities and Challenges in Implementation:*  
<http://rfidprivacy.mit.edu/access/pdfs/report-doc.pdf>

### Federal Trade Commission

*Radio Frequency Identification: Applications and Implications for Consumers:*  
<http://rfidprivacy.mit.edu/access/pdfs/report-ftc.pdf>

### Government Accountability Office

*Information Security: Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology* (GAO-05-849T) June 22, 2005:  
<http://www.gao.gov/new.items/d05849t.pdf>

*Information Security: Radio Frequency Identification Technology in the Federal Government* (GAO-05-551) May 27, 2005: <http://www.gao.gov/new.items/d05551.pdf>

### Homeland Security Department

*United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) Privacy Impact Assessment* (70 Fed. Reg. 39300, 7/7/05):  
<http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/p-13371.pdf>

### State Department

*E-Passport Final Rule* (70 Fed. Reg. 61553, 10/25/05):  
<http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/p-21284.pdf>

## INTERNATIONAL

## Article 29 Data Protection Working Party

*Working Document on Data Protection Issues Related to RFID Technology*, Jan. 19, 2005:

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp105\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf)

*Summary of Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology*, Sept. 28, 2005:

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp111\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf)

*Computing Technology Industry Association (response to the Jan. 19, 2005, Article 29 Data Protection Working Party)*:

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/rfid/comptia\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/rfid/comptia_en.pdf)

*EPCglobal (response to the Jan. 19, 2005, Article 29 Data Protection Working Party)*:

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/rfid/epcglobal\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/rfid/epcglobal_en.pdf)

*Open Business Innovation (response to the Jan. 19, 2005, Article 29 Data Protection Working Party)* March 31, 2005:

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/rfid/obi\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/rfid/obi_en.pdf)

*RSA Security (response to the Jan. 19, 2005, Article 29 Data Protection Working Party)*:

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/rfid/rsa-security-usa\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/rfid/rsa-security-usa_en.pdf)

## Canada

*RFID Technology Fact Sheet*, Office of the Privacy Commissioner of Canada:

[http://www.privcom.gc.ca/fs-fi/02\\_05\\_d\\_28\\_e.asp](http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp)

*Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, Information and Privacy Commissioner Ontario: <http://www.ipc.on.ca/docs/rfid.pdf>

## Organization for Economic Cooperation and Development

*RFID Applications and Public Policy Considerations*, Oct. 5, 2005:

[http://www.oecd.org/document/58/0,2340,en\\_2649\\_34223\\_35186234\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/58/0,2340,en_2649_34223_35186234_1_1_1_1,00.html)

## Japan

*Guidelines for Privacy Protection with Regard to RFID Tags*, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, Government of Japan, July 2004:

[http://www.meti.go.jp/english/information/data/IT-policy/pdf/guidelines\\_for\\_privacy\\_protection\\_with\\_regard\\_to\\_rfid\\_tags.pdf](http://www.meti.go.jp/english/information/data/IT-policy/pdf/guidelines_for_privacy_protection_with_regard_to_rfid_tags.pdf)

# NONGOVERNMENTAL ORGANIZATIONS

## AeA

*RFID 101: Benefits of the Next Big Little Thing*, Part 1 of a two-part analysis, December 2005: [http://aeanet.org/publications/AeA\\_CS\\_RFID\\_101.asp](http://aeanet.org/publications/AeA_CS_RFID_101.asp)

*Advancing the Business of Technology RFID: Security, Privacy, and Good Public Policy*, Part 2 of a two-part analysis, February 2006:

[http://aeanet.org/publications/AeA\\_CS\\_RFID\\_grad.asp](http://aeanet.org/publications/AeA_CS_RFID_grad.asp)

**American Hospital Association***Health IT Survey*, Oct. 6, 2005:<http://www.ahapolicyforum.org/ahapolicyforum/resources/content/FINALNonEmbITSurvey>**Citizens Against Government Waste***Through the Looking Glass: Real ID: Big Brother Could Cost Big Money*, Oct. 17, 2005:[http://www.cagw.org/site/DocServer/Real\\_ID\\_FINAL\\_with\\_cover.pdf?docID=1281](http://www.cagw.org/site/DocServer/Real_ID_FINAL_with_cover.pdf?docID=1281)**Electronic Frontier Foundation***Radio Frequency Identification (RFID)*: <http://www.eff.org/Privacy/Surveillance/RFID/>**Electronic Privacy Information Center***Radio Frequency Identification (RFID) Systems*: <http://www.epic.org/privacy/rfid/>*EPIC Comments to the Department of Homeland Security Data Privacy and Integrity Advisory Committee* (Docket No. DHS-2005-0047), Dec. 6, 2005:<http://www.epic.org/privacy/us-visit/comm120605.pdf>**IDTechEx***The RFID Knowledgebase*: <http://rfid.idtechex.com/knowledgebase/en/nologon.asp>**International Chamber of Commerce***ICC principles for responsible deployment and operation of electronic product codes*, 2005:[http://www.iccwbo.org/home/statements\\_rules/statements/2005/EPC\\_Principles.pdf](http://www.iccwbo.org/home/statements_rules/statements/2005/EPC_Principles.pdf)**International Telecommunications Union***The Internet of Things*, November 2005:<http://www.itu.int/osg/spu/publications/internetofthings/>**National Electronic Commerce Coordinating Council***RFID*: <http://rfidprivacy.mit.edu/access/pdfs/report-ec3.pdf>.**RAND Corporation***9 to 5: Do You Know if Your Boss Knows Where You Are?:*[http://www.rand.org/pubs/technical\\_reports/2005/RAND\\_TR197.pdf](http://www.rand.org/pubs/technical_reports/2005/RAND_TR197.pdf)**Security Research Group***RFID Vulnerabilities*, Edith Cowan University School of Computer and Information Science, SW Australia: <http://scissec.scis.ecu.edu.au/wordpress/>

## OTHER REPORTS & RESOURCES

**Academic Papers***"Is Your Cat Infected with a Computer Virus?"* Vrije Universiteit Amsterdam Computer Systems Group: <http://www.rfidvirus.org/papers/percom.06.pdf>*"Privacy for RFID Through Trusted Computing,"* Nov. 7, 2005:<http://www.cs.berkeley.edu/~dmolnar/papers/wpes05-camera.pdf>*"Security and Privacy Issues in E-passports,"* Ari Juels, David Molnar, and David Wagner, (SecureComm, September 2005):<http://www.cs.berkeley.edu/~dmolnar/papers/RFID-passports.pdf>

"RFID Privacy: A Technical Primer For The Non-Technical Reader" (Feb. 23, 2005 Draft),  
Ari Juels:  
[http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid\\_privacy/DePaul23Feb](http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid_privacy/DePaul23Feb)

## Vendors

VeriChip Corporation, "RFID for People": <http://www.verichipcorp.com/> 

---

Contact customer relations at: [customercare@bna.com](mailto:customercare@bna.com) or 1-800-372-1033  
ISSN 1538-3431

[Copyright](#) © 2006, The Bureau of National Affairs, Inc.  
[Copyright FAQs](#) | [Internet Privacy Policy](#) | [BNA Accessibility Statement](#) | [License](#)

Reproduction or redistribution, in whole or in part, and in any form,  
without express written permission, is prohibited except as permitted by the BNA Copyright Policy,  
<http://www.bna.com/corp/index.html#V>

 <a href="#">Search All Issues</a>	 <a href="#">Contents</a>
---	--

Toby Milgrom Levin  
Senior Advisor  
The Privacy Office  
Department of Homeland Security  
Washington, DC 20528  
*Direct: 571.227.4128*  
*Privacy Office: 571.227.3813*  
*Fax: 571.227.4171*  
**b)(2), (b)(6)**

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

## Burroughs, Sabrina

---

**From:** Mortensen, Kenneth (b)(2)(low), (b)(6)  
**Sent:** Wednesday, March 15, 2006 6:39 PM  
**To:** (b)(2), (b)(6) Kropf, John  
**Subject:** Fw: Faculty of Science Vrije Universiteit

Kenneth P. Mortensen  
Acting Chief of Staff  
Office of the Secretary, Privacy Office  
U.S. Department of Homeland Security  
-----

Sent from my BlackBerry Wireless Handheld

-----Original Message-----

**From:** (b) (6)  
**To:** Yonkers, Steve; Mortensen, Kenneth  
**Sent:** Wed Mar 15 17:04:57 2006  
**Subject:** FW: Faculty of Science Vrije Universiteit

-----Original Message-----

**From:** Mocny, Robert  
**Sent:** Wednesday, March 15, 2006 2:36 PM  
**To:** (b) (6)  
**Subject:** Faculty of Science Vrije Universiteit

<http://www.rfidguardian.org/index.html>

## Burroughs, Sabrina

---

**From:** Levin, Toby  
**Sent:** Wednesday, June 21, 2006 1:11 PM  
**To:** Mortensen, Kenneth; Kropf, John; Richards, Rebecca; Sand, Peter  
**Cc:** Cooney, Maureen  
**Subject:** Cavoukian's RFID Guidelines

[http://www.ipc.on.ca/scripts/index.asp?action=31&N\\_ID=1&P\\_ID=16983&U\\_ID=0](http://www.ipc.on.ca/scripts/index.asp?action=31&N_ID=1&P_ID=16983&U_ID=0)

Above is link to Anne Cavoukian's RFID guidelines:

### Commissioner Cavoukian issues RFID Guidelines and Practical Tips aimed at protecting privacy

NEWS RELEASE : June 19, 2006 ([PDF](#) version)

## Commissioner Cavoukian issues RFID Guidelines aimed at protecting privacy

Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, today released privacy [Guidelines](#) for the growing field of radio frequency identification (RFID).

These *Guidelines* flow from her earlier work in 2003 when the Commissioner first identified the potential privacy concerns raised by RFID technology. Following a history of ground-breaking work on building privacy into the design of emerging technologies, these *Guidelines* are a natural progression of this pragmatic approach.

"I have always found it beneficial to assist those working on emerging technologies, and to be proactive whenever possible – to develop effective guidelines and codes **before** any problems arise," said Commissioner Cavoukian. "These made-in-Canada *Guidelines* provide guidance and solutions regarding item-level consumer RFID applications and uses."

EPCglobal Canada, an industry association that sets standards for electronic product codes, has been collaborating with the IPC in the development of these *Guidelines*, and will be seeking Board approval by its member companies to signify the association's endorsement of the *Guidelines*.

"This technology offers exciting benefits to consumers and businesses alike. As the trusted source for driving adoption of EPC/RFID technology for increased visibility within the supply chain, privacy is as important as anything else we are doing," said Art Smith, President and CEO, EPCglobal Canada. "We promote an environment that encourages ongoing innovation while respecting privacy issues."

RFID tags contain microchips and tiny radio antennas that can be attached to products. They transmit a unique identifying number to an electronic reader, which in turn links to a computer database where information about the item is stored. RFID tags may be read from a distance quickly and easily, making them valuable for managing inventory but pose potential risks to privacy if linked to personal identifiers. RFID tags are the next generation technology from barcodes.

Although RFID technology deployed in the supply chain management process poses little threat to privacy, item-level use of RFID tags in the retail sector, when linked to personally identifiable information, can facilitate the tracking and surveillance of individuals. The goal of these *Guidelines* is to alleviate concerns about the potential threat to privacy posed by this technology and to enhance

openness and transparency about item-level use of RFID systems by retailers.

The *Guidelines* address key privacy issues regarding the use of RFID technology at an item-level in the retail sector, said Commissioner Cavoukian.

The *Guidelines* are based on three overarching principles, including:

- **Focus on RFID information systems, not technologies:** The problem does not lie with RFID technologies themselves, but rather, the way in which they are deployed that can have privacy implications. The Guidelines should be applied to RFID information systems as a whole, rather than to any single technology component or function;
- **Build in privacy and security from the outset – at the design stage:** Just as privacy concerns must be identified in a broad and systemic manner, so, too, must the technological *solutions* be addressed systemically. A thorough privacy impact assessment is critical. Users of RFID technologies and information systems should address the privacy and security issues early in the design stages, with a particular emphasis on data minimization. This means that wherever possible, efforts should be made to minimize the identifiability, observability and linkability of RFID data; and
- **Maximize individual participation and consent :** Use of RFID information systems should be as open and transparent as possible, and afford individuals with as much opportunity as possible to participate and make informed decisions.

A companion piece to the Guidelines – [Practical Tips for Implementing RFID Privacy Guidelines](#), is also being released by the Commissioner to help organizations put the *Guidelines* into practice.

Toby Milgrom Levin  
Senior Advisor  
The Privacy Office  
Department of Homeland Security  
Washington, DC 20528  
*Direct: 571.227.4128*  
*Privacy Office: 571.227.3813*  
*Fax: 571.227.4171*

b)(2), (b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.



## **AGENDA**

**Canada and the United States  
Border Documents and Technology Working Group Meeting  
12 December 2006  
Ottawa  
9:00 a.m. – 2:00 p.m**

---

1. Introductions, Opening remarks and objectives (US and CAN) 20 *minutes*
2. Secure Document Standards - Update on Day-Chertoff Meeting (CAN and US) -- 30 *minutes*
3. Real-time validation of documents - Explanation of DHS requirements (US) with discussion – 30 *minutes*
4. Passport Card and NEXUS RFI Interoperability (US) with discussion – 30 *minutes*
5. Information Sharing - CBSA Legal Perspective (CAN and US)- 30 *minutes*
6. New Documents - Assessment Process (CAN and US) -40 *minutes*
7. BC - Washington Pilot - Progress Report (CAN and US) 30 *minutes*
8. Modelling (CAN and US) – 20 *minutes*
9. Next steps – 10 *minutes*



## **AGENDA**

**Canada and the United States  
Technical Consultative Working Group Meeting  
Security and Prosperity Partnership - Deliverable 1.1.3  
12 December 2006**

---

1. Opening remarks and objectives
2. Secure Document Standards - Update on Day-Chertoff Meeting (CAN and US)
3. Real-time validation of documents - Explanation of DHS requirements (US)
4. Passport Card and NEXUS RFI Interoperability (US)
5. Information Sharing - CBSA Legal Perspective (CAN and US)
6. New Documents - Assessment Process (CAN and US)
7. BC - Washington Pilot - Progress Report (CAN and US)
8. Modelling (CAN and US)
9. Next steps