

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/pr-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/pr-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

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

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

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

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

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

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

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

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

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

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

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**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**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**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

Vendors

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

Contact customer relations at: 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>

 Search All Issues	 Contents
---	--

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)(low), (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: 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)(low), (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: Ballard, Shannon (b)(2)(low), (b)(6)
Sent: Wednesday, October 18, 2006 3:09 PM
To: Kropf, John; Saadat, Lauren
Subject: EC press release on RFID

Radio Frequency Identification Devices (RFID): Frequently Asked Questions on the Commission's Public Consultation

Reference: MEMO/06/378 Date: 16/10/2006

HTML: EN
PDF: EN
DOC: EN

MEMO/06/

Brussels, 16 October :

Radio Frequency Identification Devices (RFID): Frequently Asked Questions on the Commission's Public Consultation

The European Commission today reports on the initial findings from its wide public debate on Radio Frequency Identification. At the 'RFID – Heading for the Future' conference in Brussels today, possible future policy options will be discussed with stakeholders from all over Europe and beyond.

Why this conference?

The EU RFID Conference 2006 'Heading for the Future' closes the series of radio frequency identification (RFID) consultations launched by Viviane Reding, Commissioner for Information Society and Media, at CeBIT 2006.

Why is RFID on the European Commission's agenda?

The Commission considers RFID as an emerging technology that has great potential for many economic operators in Europe as well as for Europe's citizens. Few new technologies have triggered so much attention from businesses, consumer organisations, data protection experts and politicians around the world as RFID Devices. The place taken by RFID in the public debate today largely derives from the fact that this technology is currently moving rapidly from the research lab to mass applications in a similar way to GSM mobile phones in the 1990s.

The RFID market is expected to grow rapidly over the next ten years. Cumulative sales worldwide of RFID tags for 60 years since their invention until the beginning 2006 amount to 2.4 billion, with 600 million tags being sold in 2005 alone! The number of tags delivered in 2016 could be over 450 times the number delivered in 2006. If the main technical and economic challenges are resolved in the near future (e.g., yield vs. cost, frequency acceptance, required performance levels), the global RFID market might grow exponentially to be almost ten times the size in 2016 than will be this year – the value of the total market, including systems and services, could reach 20.8 billion euro in 2016 from 2.2 billion euro in 2006.

In Europe, RFID take-up growth for the next seven years is expected to be significant in the number of tags (by a factor of 6), the number of readers (by a factor of 15) and the number of locations (by a factor of 15). Yet the European RFID market is currently growing slower than the worldwide market.

The deployment of RFID technology should make a major contribution to growth and jobs. Furthermore, RFID implementations are expected to become a source of new business models and a creator of high-tech quality jobs.

At the same time, research must be pursued to build and maintain Europe's lead in next-generation RFID technology and its applications. The Commission also expects RFID to be the forerunner of many increasingly "intelligent" objects that interact with each other and help humans in ever more sophisticated ways.

Why is the Commission involved in RFID? Why not leave it completely to the private sector?

The private sector is crucial for developing the technological and economic conditions for successfully introducing RFID technologies. But as the private sector cannot clear all the roadblocks, this could slow RFID introduction.

Examples include the need for a common European technical standard to ensure that RFID systems work together and the lack of a radio frequency allocation common to all EU Member States. Suitable standards for RFID are crucial to its successful introduction. The Commission relies on standards proposed by the existing standardisation bodies in Europe, such as CEPT and ETSI for frequency spectrum

allocation, and CEN and ISO for interoperability. It counts on self-regulation and industry-wide agreements to remove the remaining obstacles.

RFID also raises a number of public interest issues, including data protection and security. Here, there is a clear need to identify joint European responses to legitimate societal concerns. On privacy, RFID is generating a number of important questions such as: how do we credibly ensure that RFID tags are not abused to invade the privacy of consumers? Do we need to destroy an RFID tag when it could be useful self-configuring products (built from autonomous components and assemblies), automating warranty checks etc.? The Commission's role here is to help build a societal consensus on technical, legal and ethical issues associated with RFID and to intervene, where required, with regulatory instruments.

In addition to privacy, the interoperability debate and the availability of radio frequency spectrum are also important. We very much need a common approach throughout Europe, so as to ensure that individual EU Member States do not opt for incompatible solutions which ultimately would be detrimental to everyone. For example, because Europe lacks a common frequency range for ultra-high frequency (UHF) tags, electronic invoicing is possible within each country, but e-invoicing systems will not work across borders. Also a sector-specific approach, such as common EU guidelines that set out minimal requirements for RFID applications in different sectors (such as healthcare or government), might be helpful for industry and citizens in Europe.

Why did the European Commission hold consultations on RFID?

The Commission launched this consultation process to give all stakeholders a chance to express their concerns. This will help the Commission to decide on the steps that Europe must take to seize the opportunities offered by RFID, and to address the complex issues of security and privacy that surround it. The results of the public consultation will feed into a Commission Communication to the Council and the European Parliament that the Commission intends to adopt at the end of 2006.

How did the European Commission organise this consultation?

As a first step, the European Commission held five workshops with experts and stakeholders from Europe and around the world on:

- technological state of RFID development (6 and 7 March 2006);
- economic and social rationale for RFID applications domains and emerging trends (15 and 16 May 2006);
- RFID security, privacy, health and safety issues (16-17 May 2006);
- RFID interoperability, standardisation, governance and Intellectual Property Rights (1 June); and

- RFID radio frequency requirements (2 June 2006).

The workshops featured 128 distinguished speakers and attracted 623 external participants. In addition, remote access to the conference with web-streaming of presentations and the possibility to submit questions was made available in four workshops (see

http://europa.eu.int/information_society/policy/rfid/workshops/index_en.htm).

To further the debate, an online public consultation asked stakeholders for their opinion on how the European Commission could ensure that the growing use of RF boosts the competitiveness of Europe's economy and improves quality of life. It was held on 'Your Voice in Europe' from 3 July until 30 September 2006 and enjoyed unexpected high participation from stakeholders in Europe and worldwide (see http://europa.eu.int/information_society/policy/rfid/consultation/index_en.htm).

[Figures and graphics available in PDF and WORD PROCESSED]

What have been the key issues raised during the public consultation?

The key issues addressed in the debate so far have included: (i) the migration from today's RFID tags to the vision of creating an 'Internet of Things' via networked RFID systems and services; (ii) emerging trends and opportunities in RFID application domains; (iii) RFID security, data protection and privacy, health and safety issues (iv) interoperability, standardisation, governance, and intellectual property rights; (v) radio frequency requirements for RFID.

Besides technical issues, the debate has highlighted the need to address key social concerns. These include the privacy risks of collecting and using personally-identifying information (e.g., data mismanagement, data misuse, lack of transparency, loss of freedom), but also the biological effects of radio frequency waves and the impact of RFID tags on packaging materials reuse and recycling.

The Commission's debate raised stakeholder awareness of the economic and social benefits of RFID technology, and identified policy options to respond to the citizen-specific concerns. The Commission is examining the need to promote a regulatory environment in which RFID users can develop robust, high-performance applications but which at the same time ensures that the right to privacy is fully protected.

Did many participate in the Commission's public RFID consultation?

The online public consultation, which the Commission launched on 3 July (see [IP/06/909](http://europa.eu.int/rapid/press_releases_fre.htm?PRIP/06/909)) and which ended on 17 September 2006, caught the attention of many citizens and organisations: 2190 respondents - a record for such consultations - submitted the questionnaire. All consultation documents can be accessed at <http://www.rfidconsultation.eu/>

Where are we today with respect to radio spectrum?

Currently the main issue is the regulations for using RFID technology in the ultra high frequency (UHF) range from 865-868 MHz. Transponders constructed for this range are less expensive and can be read much more quickly and over distances of many metres. To provide a consistent RFID environment throughout the European Union the Commission took the initiative to ensure legal certainty regarding the spectrum range and usage conditions as formulated in the ERC (European Radio Committee Recommendation 70-03

(<http://www.ero.dk/documentation/docs/doc98/official/pdf/REC7003E.PDF#search=22%22erc%20recommendation%2070-03%22%22>).

On 4 October 2006 the Radio Spectrum Committee expressed a positive opinion on the proposed Commission Decision on harmonising Spectrum in Europe for RFIDs in the UHF band. This draft Decision is expected to be formally adopted by the end of 2006. Possible further spectrum needs beyond this frequency band can be addressed in the future, after a careful assessment of the needs actually arising from RFID applications.

Will Europe further stimulate research and innovation on RFID?

Collaborative R&D has been undertaken since 2002, with some 50 projects addressing:

- the development of new RFID technologies (data carrier technology, systems technology, air-interface, communications and coding, etc.);
- the development of innovative applications in certain areas and sectors (industry and services, consumer goods, the forest-wood supply chain, etc.);
- socio-economic research;
- and pre-normative research (i.e. developments in regulations and standards for RFID at European and international level).

Research work on RFID technologies and applications will continue to integrate RFID with other enabling technologies, such as sensors, ambient intelligence and nanotechnology. At the same time, large-scale pilots for the application of RFID will be promoted, for example in hospitals, government, logistics and production. This will be part of the Commission's new Competitiveness and Innovation framework Program (2007-2013) (see

http://ec.europa.eu/enterprise/enterprise_policy/cip/index_en.htm).

How important is the international dimension of the RFID debate?

Many of the interesting RFID application areas are not limited to the European Union. Each day large amounts of goods are shipped to (and from) the United States and Asia, so common standards and rules would be more than welcome. Europe and it

key trading partners have a clear mutual interest in this area. The European Commission is and intends to remain a strong partner in the international debate. Many international working groups share the commitment to anticipating, and meeting economic and social needs with compatible and interoperable solutions. In this respect, the "Initiative to Enhance Transatlantic Economic Integration and Growth" launched by the June 2005 EU-US Summit, the EU-Japan Information Society Dialogue, or the EU-China Information Society Dialogue offer good prospects for developing joint measures to accelerate the deployment of key innovative technologies such as RFID devices.

What does Europe do today to ensure the privacy of its citizens regarding RFID?

There is a strong concern that the large-scale use of RFID technology may breach consumer's right to privacy. It is therefore not surprising that many consumer protection organisations have been very active in alerting consumers.

The European Commission has long been aware of civil rights concerns to do with information and communication technologies. EU law addresses these concerns via the Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data (95/46/EC) of 1995 (see http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm).

In May 2006, the Commission held a specific workshop on privacy and security aspects of RFID to identify real privacy concerns, and try to build consensus on effective and balanced answers. The Commission intends to promote further consultations and negotiations between all stakeholders on the privacy protection issue, taking into account the ongoing work carried out by the Article 29 Data Protection Working Party.

On the basis of the public consultation, the Commission Communication on RFID, planned for the end of 2006, will outline, if necessary, where further legislative intervention or clarifications of the existing legal framework could be necessary. This could lead to formal proposals in 2007.

More information on the public debate on RFID can be found at:
www.rfidconsultation.eu

See also [SPEECH/06/597](#)

Burroughs, Sabrina

From: Slomovic, Anna (b)(2)(low),
(b)(2)(low), (b)(6)(b)(2)(low), (b)(6)(b)(2)(low), (b)(6)(b)(2)(low), (b)(6)(b)(2)(low), (b)(6)
Sent: Wednesday, October 19, 2005 11:38 AM
To: Privacy Office
Subject: Real ID

Interesting article on REAL ID

http://www.cagw.org/site/PageServer?pagename=reports_realid&printer_friendly=1

Burroughs, Sabrina

From: Sand, Peter (b)(2)(low), (b)(6)
Sent: Wednesday, November 16, 2005 10:03 AM
To: Kropf, John; Mortensen, Kenneth <CTR>
Subject: RE: California RFIDs?

John,

Here's an article from 11-01-2005, from www.secureidnews.com:

California RFID ban shelved ... awaiting its next round in the New Year
Tuesday, November 1 2005
By Marisa Torrieri
Contributing Editor, AVISIAN Publications
<http://www.secureidnews.com/library/2005/11/01/california-rfid-ban-shelved-awaiting-its-next-round-in-the-new-year/>

Those waiting for the 'California Gold Rush' to RFID and contactless-enabled ID cards will have to cross their fingers and sit tight. Come January 1, a new bill barring wireless identification technology in government-issued IDs, authored by California Senator Joe Simitian (D-Palo Alto) will hit the state's legislative floor. Should the bill pass, it would place a three-year moratorium on the use of RFID (and related technologies such as contactless smart cards) in driver licenses, K-12 ID cards, library cards, and health cards. Additionally, it would require costly and according to some, less-than-necessary, security additions to all cards.

These include encryption and mutual authentication techniques for all cards whether they include any personal data or simply a unique ID number. Additionally, the use of a shield to protect against unintended access is likely. Finally, it would restrict the expansion -- both in terms of new populations and new applications -- of any existing government RFID project.

The Identity Information Protection Act of 2005 is co-sponsored by the ACLU (American Civil Liberties Union) and the EFF (Electronic Frontier Foundation).

Should the bill pass, many in the ID card space may have to wait at least three years before the fruits of their labor can flourish. The moratorium is intended for chip-based wire- less technology to be studied more carefully before vendors can market such cards to California government agencies, according to reports.

But critics call it reactionary and unfounded. "Don't ban technology, ban bad behavior," said Marc-Anthony Signorino, director and counsel of technology policy for the AeA (formerly the American Electronics Association). "That's always been our mantra."

What's worse, from the perspective of industry, is that a three-year ban could mean the loss millions of dollars -- and not just from government contracts. Technologists who already invested in R&D may be forced to scratch current designs to incorporate mandated, higher-security chips and readers. Such technology is much more costly to produce and could raise the cost of a card from \$1 to at least \$7 each, says Mr. Signorino.

More importantly, the higher security and cost is considered unnecessary by many observers - at least for basic functions such as simple access control. Throughout the country and the world, millions of contactless smart cards and other wireless-communication IDs have been used safely and effectively.

The legislation as it stands today

Today's Identity Information Protection Act looks nothing like the original. It's gone through several revisions, most recently, a legislative process referred to as "gutting." This gutting has allowed sponsors to get the bill the equivalent of a VIP pass to the California legislative floor on Jan. 1. The gutting process has stripped the contents of what was formerly SB 682 (Senator Simitian's original bill) and dumped into another non-technology bill that had already been slated for review. Ironically, the gutted bill dealt not with RFID but fish (the "Marine Finfish Aquaculture Bill"). So come January, SB 768 will be the new number to watch.

Despite this clever maneuvering, Mr. Signorino says he is confident the bill - as it stands now - will not pass because it is flawed in several ways. For one, it puts a negative stigma on technology, and tells the public that it is not secure. In addition, it bans technology that could truly help consumers.

The AeA has offered to work out a mutual solution with Mr. Simitian's staff, which would include recommending best practices for companies and the government organizations. For example, such best practices might include rules to protect consumers (i.e., requiring an agency to ensure that a card has high enough security to guard against hacking).

Companies most affected by the bill's passing are certainly nervous about its passage and are working to convince state government officials of the merits of wireless identification technology. According to Christoph Liedtke, a spokesman for smartcard/contactless card manufacturer Infineon Technologies, the key is to educate the parties that there is significant difference between the less-secure RFID that is used to track goods shipped to Wal-Mart and the chip technology intended for ID cards.

"What we are talking about when we're talking about contactless technology is an extremely secure technology, that stores encrypted information on a chip," says Mr. Liedtke. "It's a much safer technology than the existing magnetic stripe."

The general industry perception seems to be that while it is always good to evaluate the potential impacts of a technology, it is not wise to react based on fear. As Mr. Liedtke points out, "it's the skimming and eavesdropping that (many) fear. We share the concern of privacy - but don't share concern that existing technology is insecure."

But supporters of the bill, say arguments like Mr. Liedtke's are just plain old propaganda.

"In a 12-step program, one of the first things you have to do is go from denial to acceptance that you have a problem," says Lee Tien, senior staff attorney for bill co-sponsor EFF. "The RFID industry is still in denial."

Mr. Tien says companies in the ID card space need to show that they are concerned about privacy, and willing to employ technology in a socially responsible way, for example, by working on pilots and improving their designs so the technology is more "privacy protected."

Mr. Tien also said he is skeptical of the much higher cost per card of deploying such technology. "I would like to see what those numbers are based on," says Mr. Tien, adding that, "when you do something in volume, the cost goes down."

For now, California is the only state that is pushing for such a bill, says Mr. Signorino. But because of its sheer size, a ban on RFID and similar technologies would be a sweeping loss. According to Mr. Signorino, in the state of California, 23 million people have driver licenses; 3.5 million have identification cards, and that is just the tip of the iceberg.

"Right now we're trying to build up education, working with different legislators," Mr. Signorino says, "letting them know what should be done to protect consumers' privacy."

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

From: Kropf, John [mailto:(b)(2)(low), (b)(6)]
Sent: Wednesday, November 16, 2005 9:37 AM
To: Sand, Peter; Mortensen, Kenneth <CTR>
Subject: California RFIDs?

Are either of you aware of a California law that applies specifically RFIDs? We took a question from a member of the German Parliament on this point during on our trip and anything you can provide would be helpful in answering the mail.

Thanks.

If so, can we say I wish all could California RFIDs (this will only work if you think of the Beach Boys Song).

John Kropf

Director of International Privacy Programs

DHS, Privacy Office

Tel. 571-227-3813

Fax: 571-227-4171

Email (b)(2)(low), (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 received this in error, please reply immediately to the sender and delete the message. Thank you.

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

reported in

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)(low), (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: Mortensen, Kenneth (b)(2)(low), (b)(6)
Sent: Wednesday, March 15, 2006 6:39 PM
To: (b)(2)(low), (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>

Security
 Experts Respond To Tracking Technology Concerns
 by Winter Casey

Despite new research pointing to security vulnerabilities in wireless tracking technology known as radio-frequency identification, government and business representatives remain confident in its use.

Last week, a study from Amsterdam's Vrije University warned that computer viruses could move from RFID tags to exploit some software systems. The research -- "Is Your Cat Infected with a Computer Virus?" by Melanie Rieback -- was presented at the Institute of Electrical and Electronics Engineers conference in Pisa, Italy.

RFID software code writers must build appropriate checks "to prevent RFID middleware from suffering all of the well-known vulnerabilities experienced by the Internet," according to the report. The paper claims to present the first self-replicating RFID virus.

Governments and businesses around the world have been adapting applications of RFID for various tasks, such as tracking groceries or cargo and verifying people's identities.

A State Department official said the United States plans to begin deploying new passports with RFID technology on a widespread basis this summer. The number of passports being issued over the past few years has increased from 7.3 million in fiscal 2003 to more than 13 million expected to be issued in 2006.

"The security of the e-passport is of the utmost importance to the State Department. We only went ahead in issuing them after ensuring that the data would be protected," said the official, who noted that the passport includes a different type of RFID than the one questioned in the report. To address privacy concerns, the State Department has added technology to prevent the inappropriate "skimming" of passport data by other technology in the vicinity. Privacy advocate Bill Scannell labeled the move "considerably better than nothing."

Dan Mullen, president of the identification trade association AIM Global, said in a statement that many of the paper's assumptions "overlook a number of fundamental design features necessary in automatic data-collection systems and good database design." A representative for the RFID company Alien Technology agreed.

But the technology has some privacy advocates concerned. "There is absolutely no need to use an RFID technology," said Scannell, who added that "relying on RFID for security is a bad idea."

RFID "works well for cattle but not for people," Scannell said in reference to the use of the technology in livestock for tracking purposes.

Evan Scott, the president of Evan Scott Group International, said he has confidence in the system and works with RFID companies on a daily basis. "A lot is being done every day to ensure security," he said.

"There are risk and concerns with all technology," said Scott, who noted that the concerns drive research and development. "RFID issues will be resolved and fixed through good technology. We are in the information age now. Everything is on the Internet or through the airwaves."

A lot of venture-capital investments have been going toward RFID in the last couple years, Scott noted. He expects the trend to continue with more commercial and security applications.

RFID tags vulnerable to viruses, study says
 Attacks could soon come in the form of a SQL injection or a buffer overflow attack
http://www.computerworld.com/securitytopics/security/story/0,10801,109560,00.html?source=NLT_PM&nid=109560

News Story by Jeremy Kirk
 (Embedded image moved to file: pic27967.gif)
 MARCH 15, 2006 (IDG NEWS SERVICE) - Three computer science researchers are warning that viruses embedded in radio tags used to identify and track goods are right around the corner, a danger that so far has been overlooked by the industry's high interest in the technology.

No viruses targeting radio frequency identification (RFID) technology have been released live yet, according to the researchers at Vrije Universiteit Amsterdam in the Netherlands. But RFID tags have several characteristics that could be engineered to exploit vulnerabilities in middleware and back-end databases, they wrote in a paper presented today at a conference in Pisa, Italy.

"RFID malware is a Pandora's box that has been gathering dust in the corner of our 'smart' warehouses and home," the paper stated.

The attacks can come in the form of a SQL injection or a buffer overflow attack even though the tags themselves may only store a small bit of information, the paper said. For demonstration purposes, the researchers created a proof-of-concept, self-replicating RFID virus.

Patrick Simpson, a master's student at the university, needed only four hours to write a virus small enough to fit on a RFID tag, something previously thought unworkable, said Andrew S. Tanenbaum, a professor at Vrije Universiteit Amsterdam. RFID tags can contain as little as 114 bytes of memory, he said.

Tanenbaum expects vendors to be angry about the publishing of the code. Vendors have dismissed the possibility of RFID viruses, saying that the amount of memory in the tags is too small, he said.

But the researchers did take precautions to ensure RFID viruses won't immediately circulate. They wrote their own middleware that mimicked traits of products on the market, said Melanie R. Rieback, one of the paper's authors.

"It's not like we are providing a cookbook for basically wannabe hackers to hack real RFID systems," Rieback said.

The homespun middleware connected to back-end databases from vendors such as Oracle Corp. and Microsoft Corp. along with open-source databases such as MySQL and Postgres, Rieback said. The experiment used RFID equipment from Philips Electronics NV, she said.

"It was actually quite interesting to see that some of the databases were susceptible to some kinds of attacks," Rieback said. "Other ones actually had natural protection mechanisms built in that made them more resistant."

Page 2 of 2

The purpose of the exercise, the authors wrote, is to encourage RFID middleware designers to be more careful when writing code. Back-end middleware can contain millions of lines of source code, and if software faults number between six and 16 per 1,000 lines of code, the programs are likely to have many vulnerabilities, the paper said.

RFID tags are increasingly being used in a variety of industries to track items and give a real-time view of inventories. The tags contain data on a particular object or, in some cases, embedded in animals, and that data is typically stored in a database.

Companies can save money by using the tags to keep closer tabs on their property. However, this "pervasive computing utopia has its dark side," the authors wrote.

RFID systems may be attractive to criminals since the data contained on them may have a financial or personal nature, such as information stored on digital passports. In addition to causing damage to computer systems, RFID malware may have an effect on real-world objects, the paper said.

For example, airports are considering using RFID tags to track baggage. But Tanenbaum warned that this application could pose a large problem if an RFID tag is read and delivers a much larger set of data in return. A false tag on a piece of baggage could exploit a buffer overflow to deliver a virus to the RFID middleware. Once the virus code is on the server, it could infect the databases and corrupt subsequent tags or install back doors -- small programs that allow for the extrication of data over the

Internet, Tanenbaum said.

"You can hide baggage," Tanenbaum said. "You can reroute baggage to the wrong place -- all kinds of mischief. That's I think a very, very serious thing that even has national security implications."

Related Opinion:

IT Blogwatch: RFID malware demonstrated (and DIY axis of crypto)

ID tags vulnerable to viruses, study finds olsonss@state.gov
By John Markoff The New York Times

WEDNESDAY, MARCH 15, 2006

A group of European computer researchers has demonstrated that it is possible to insert a software virus into radio frequency identification tags, part of a microchip-based tracking technology in growing use in commercial and security applications.

In a paper that was being presented Wednesday at an academic computing conference in Pisa, Italy, the researchers demonstrate how it is possible to infect a tiny portion of memory in the chips that is often large enough to hold only 128 characters of information.

Until now, most computer security experts have discounted the possibility of using such tags, known as RFID chips, to spread a computer virus because of the tiny amount of memory on the chips.

The tracking systems are intended to improve the accuracy and lower the cost of tracking goods in supply chains, warehouses and stores. Radio tags store far more data about a product than bar codes and can be read more quickly. They have even been injected into pets and livestock for identification.

The chips have already prompted debate over privacy and surveillance, given their tracking ability. Now the researchers have added a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the future.

In the researchers' paper - "Is Your Cat Infected With a Computer Virus?" - the group, affiliated with the computer science department at the Free University in Amsterdam, also describes how the vulnerability could be used to undermine a variety of tracking systems.

The researchers said they realized there were risks associated with publishing security vulnerabilities in computerized systems. To head off some of the possible attacks they described, they have also published a set of steps to help protect RFID chips from such attacks.

The group, led by Andrew Tanenbaum, an American computer scientist, was making the presentation at the annual Pervasive Computing and Communications Conference sponsored by the Institute of Electrical and Electronic Engineers. Tanenbaum is the author of the Minix operating system, an experimental project that became the heart of the Linux open-source operating system.

The researchers asserted that the RFID demonstration had not used the commercial software that collects and organizes information from RFID readers. Rather, it used software that they had designed to replicate those systems.

"We have not found specific flaws" in the commercial RFID software, Tanenbaum said, but "experience shows that software written by large companies has errors in it." The researchers have posted their paper and related materials on security issues related to RFID systems at www.rfidvirus.org.

The researchers acknowledged that inside information would be required in many cases to plant a hostile program. But they asserted that the

commercial software developed for RFID applications potentially had the same vulnerabilities previously exploited by viruses and other malicious software, or malware, in the rest of the computer industry.

One such standard industry problem is a software coding error referred to as a buffer overflow. Such errors occur when programmers set aside memory to receive data temporarily but fail to require a check on the size of the value that is moved to the allocated space. A larger-than-expected value can cause the program to break and trick the computer operating system into executing a malicious program.

"You should check all of your input all of the time, but experience shows this isn't the case," Tanenbaum said.

Independent computer security specialists also said RFID systems were potential problem areas.

"It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever," said Peter Neumann, a computer scientist at SRI International, a research firm in Menlo Park, California.

Neumann is the co-author of an article to be published in the May issue of the Communications of the Association for Computing Machinery on the risks of RFID systems. He said existing RFID systems were a computer security disaster waiting to happen.

He cited inadequate identification for users, the potential for counterfeiting or disabling tags and the problem of weak encryption in a passport-tracking system being developed in the United States. But he said he had not previously considered the possibility of viruses and other malicious software programs.

An industry executive acknowledged that the companies that make computerized tracking systems faced potential security problems.

"We are very actively looking at the different way the technology is used," said the executive, Daniel Mullen, president of the Association for Automatic Identification and Mobility, an industry trade group. "It's an ongoing dialogue about protecting information on the tag and in the database."

The association has a working group of experts assessing both security and privacy challenges, he said.

There are many types of RFID tag, and some of the sophisticated versions include security features like encryption of the identifying number carried by the chip. But the Dutch research group warned that in a variety of situations it was possible for attackers to alter the information in an RFID tag to subvert its purpose.

"RFID malware is a Pandora's box that has been gathering dust in the corners of our 'smart' warehouses and homes," they write in their paper.

In one example they offered, a virus from an infected tag on luggage passing through an airport could be picked up when it is scanned by the luggage-handling control systems and then spread to tags attached to other pieces of luggage.

Such an attack, they suggest, might spread luggage contamination to other airports. It might also be used by a smuggler to cause a piece of luggage to avoid security systems. They also described situations of counterfeit RFID tags possibly being used to subvert pricing and other aspects of commercial sales systems or of a virus's being inserted into RFID tags used to identify pets.

A group of European computer researchers has demonstrated that it is possible to insert a software virus into radio frequency identification tags, part of a microchip-based tracking technology in growing use in commercial and security applications.

In a paper that was being presented Wednesday at an academic computing conference in Pisa, Italy, the researchers demonstrate how it is possible to infect a tiny portion of memory in the chips that is often large enough to hold only 128 characters of information.

Until now, most computer security experts have discounted the possibility of using such tags, known as RFID chips, to spread a computer virus because of the tiny amount of memory on the chips.

The tracking systems are intended to improve the accuracy and lower the cost of tracking goods in supply chains, warehouses and stores. Radio tags store far more data about a product than bar codes and can be read more quickly. They have even been injected into pets and livestock for identification.

The chips have already prompted debate over privacy and surveillance, given their tracking ability. Now the researchers have added a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the future.

In the researchers' paper - "Is Your Cat Infected With a Computer Virus?" - the group, affiliated with the computer science department at the Free University in Amsterdam, also describes how the vulnerability could be used to undermine a variety of tracking systems.

The researchers said they realized there were risks associated with publishing security vulnerabilities in computerized systems. To head off some of the possible attacks they described, they have also published a set of steps to help protect RFID chips from such attacks.

The group, led by Andrew Tanenbaum, an American computer scientist, was making the presentation at the annual Pervasive Computing and Communications Conference sponsored by the Institute of Electrical and Electronic Engineers. Tanenbaum is the author of the Minix operating system, an experimental project that became the heart of the Linux open-source operating system.

The researchers asserted that the RFID demonstration had not used the commercial software that collects and organizes information from RFID readers. Rather, it used software that they had designed to replicate those systems.

"We have not found specific flaws" in the commercial RFID software, Tanenbaum said, but "experience shows that software written by large companies has errors in it." The researchers have posted their paper and related materials on security issues related to RFID systems at www.rfidvirus.org.

The researchers acknowledged that inside information would be required in many cases to plant a hostile program. But they asserted that the commercial software developed for RFID applications potentially had the same vulnerabilities previously exploited by viruses and other malicious software, or malware, in the rest of the computer industry.

One such standard industry problem is a software coding error referred to as a buffer overflow. Such errors occur when programmers set aside memory to receive data temporarily but fail to require a check on the size of the value that is moved to the allocated space. A larger-than-expected value can cause the program to break and trick the computer operating system into executing a malicious program.

"You should check all of your input all of the time, but experience shows this isn't the case," Tanenbaum said.

Independent computer security specialists also said RFID systems were potential problem areas.

"It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever," said Peter Neumann, a computer scientist at SRI International, a research firm in Menlo Park, California.

Neumann is the co-author of an article to be published in the May issue of the Communications of the Association for Computing Machinery on the risks of RFID systems. He said existing RFID systems were a computer security disaster waiting to happen.

He cited inadequate identification for users, the potential for counterfeiting or disabling tags and the problem of weak encryption in a passport-tracking system being developed in the United States. But he said he had not previously considered the possibility of viruses and other malicious software programs.

An industry executive acknowledged that the companies that make computerized tracking systems faced potential security problems.

"We are very actively looking at the different way the technology is used," said the executive, Daniel Mullen, president of the Association for Automatic Identification and Mobility, an industry trade group. "It's an ongoing dialogue about protecting information on the tag and in the database."

The association has a working group of experts assessing both security and privacy challenges, he said.

There are many types of RFID tag, and some of the sophisticated versions include security features like encryption of the identifying number carried by the chip. But the Dutch research group warned that in a variety of situations it was possible for attackers to alter the information in an RFID tag to subvert its purpose.

"RFID malware is a Pandora's box that has been gathering dust in the corners of our 'smart' warehouses and homes," they write in their paper.

In one example they offered, a virus from an infected tag on luggage passing through an airport could be picked up when it is scanned by the luggage-handling control systems and then spread to tags attached to other pieces of luggage.

Such an attack, they suggest, might spread luggage contamination to other airports. It might also be used by a smuggler to cause a piece of luggage to avoid security systems. They also described situations of counterfeit RFID tags possibly being used to subvert pricing and other aspects of commercial sales systems or of a virus's being inserted into RFID tags used to identify pets.

Douglas E. Devereaux
Senior Policy Analyst
Office of Technology Policy
U.S. Department of Commerce
Room (b) (6)
Washington, D.C. 20230
202-482-3367
FAX 202-501-6054
FAX 202-482-6275
Doug.Devereaux@technology.GOV