

We are working on a new release of materials that includes the audio files of the press conference. Thanks to all the people interested in following up the case, we will keep you informed.

We are translating the report to different languages, we have translated already to english, spanish and swedish. Mail us if you can translate the information presented in this website. Thanks!

---

## **THE PHYSICAL ACCESS SECURITY TO WSIS: A PRIVACY THREAT FOR THE PARTICIPANTS.**

[\[IN PICTURES\]](#)

**PRESS RELEASE, Immediate distribution**

**URL: <http://www.contra.info/wsis> | [wsis@contra.info](mailto:wsis@contra.info)**

### **PRESS CONFERENCE**

**Friday 12th December 2003 at 11.30 am**

**à « La Pastorale », Route de Ferney 106 à Genève**

**[http://www.pressclub.ch/archives/events\\_2003/event\\_121203\\_1130.htm](http://www.pressclub.ch/archives/events_2003/event_121203_1130.htm)**

[\[Press Release English PDF\]](#) - [\[Nota Prensa en Castellano\]](#)

- **Ass. Prof. Dr. Alberto Escudero-Pascual**, Researcher in Computer Security and Privacy, Royal Institute of Technology, Stockholm, Sweden (EN, SP) Tel: + 41786677843 , +46 702867989 - **Stephane Koch**, President Internet Society Geneva, Executive Master of Economic Crime Investigations, Geneva, Switzerland. (FR, EN) Tel: +41 79 607 57 33 - **George Danezis**, Researcher in Privacy Enhancing Technologies and Computer Security, Cambridge University, UK. (FR, EN, GR)

### **GENEVA, 10th DEC 2003**

An international group of independent researchers attending the World Summit on the Information Society (WSIS) has revealed important technical and legal flaws, relating to data protection and privacy, in the security system used to control access to the UN Summit. The system not only fails to guarantee the promised high levels of security but also introduces the very real possibility of constant surveillance of the representatives of the civil society.

During the course of our investigation we were able to register for the Summit and obtain an official pass by "just" showing a fake plastic identity card and being photographed (via a webcam), with no other document or registration number required to obtain the pass. The limited personal data required to produce the fake ID and thus register was easily obtained - a name from the WSIS website of attendees.

However this is only half of the story.



[More photos of the WSIS Access Control](#)

The official Summit badges, which are plastic and the size of a credit card, hide a "RF smart card" [1] - a hidden chip that can communicate its information via radio frequency. It carries both a unique identifier associated with the participant, and a radio frequency tag (RFID) that can be "read" when close to a sensor. These sensors can be located anywhere, from vending machines to the entrance of a specific meeting room allowing the remote identification and tracking of participants, or groups of participants, attending the event.

The data relating to the card holder (personal details, access authorization, account information, photograph etc.) is not stored on the smart card itself, but instead managed by a centralized relational database. This solution enables the centralized system to monitor closely every movement of the participants at the entrance of the conference center, or using data mining techniques, the human interaction of the participants and their relationship. The system can potentially be extended to track participants' movements within the summit and detect their presence at particular session.

Because all of the personal data is stored in a centralized database, any part of the database can be replicated locally, or transferred to future events - for example the next WSIS Summit hosted by the Tunisian authorities in 2005.

During the registration process we requested information about the future use of the picture and other information that was taken, and the built-in functionalities of the seemingly innocent plastic badge. No public information or privacy policy was available upon our demands, that could indicate the purpose, processing or retention periods for the data collected. The registration personnel were obviously not properly informed and trained.

Our main concern is not only that the Summit participants lack information about the functionalities of this physical access system implemented, or that no one was able to answer questions of how the personal data would be treated after the Summit. The big problem is that system also fails to guarantee the promised high levels of security while introducing the possibility of constant surveillance of the representatives of civil society, many of whom are critical of certain governments and regimes. Sharing this data with any third party would be putting civil society participants at risk, but this threat is made concrete in the context of WSIS by considering the potential impact of sharing the data collected with the Tunisian government in charge of organizing the event in 2005.

That a system like this gets implemented without a transparent and open discussion amounts to a real threat for the participants themselves, and for our Information Society as a whole.

More information is available at:  
<http://www.contra.info/wsisis>  
[wsisis@contra.info](mailto:wsisis@contra.info)

## NOTES TO EDITORS

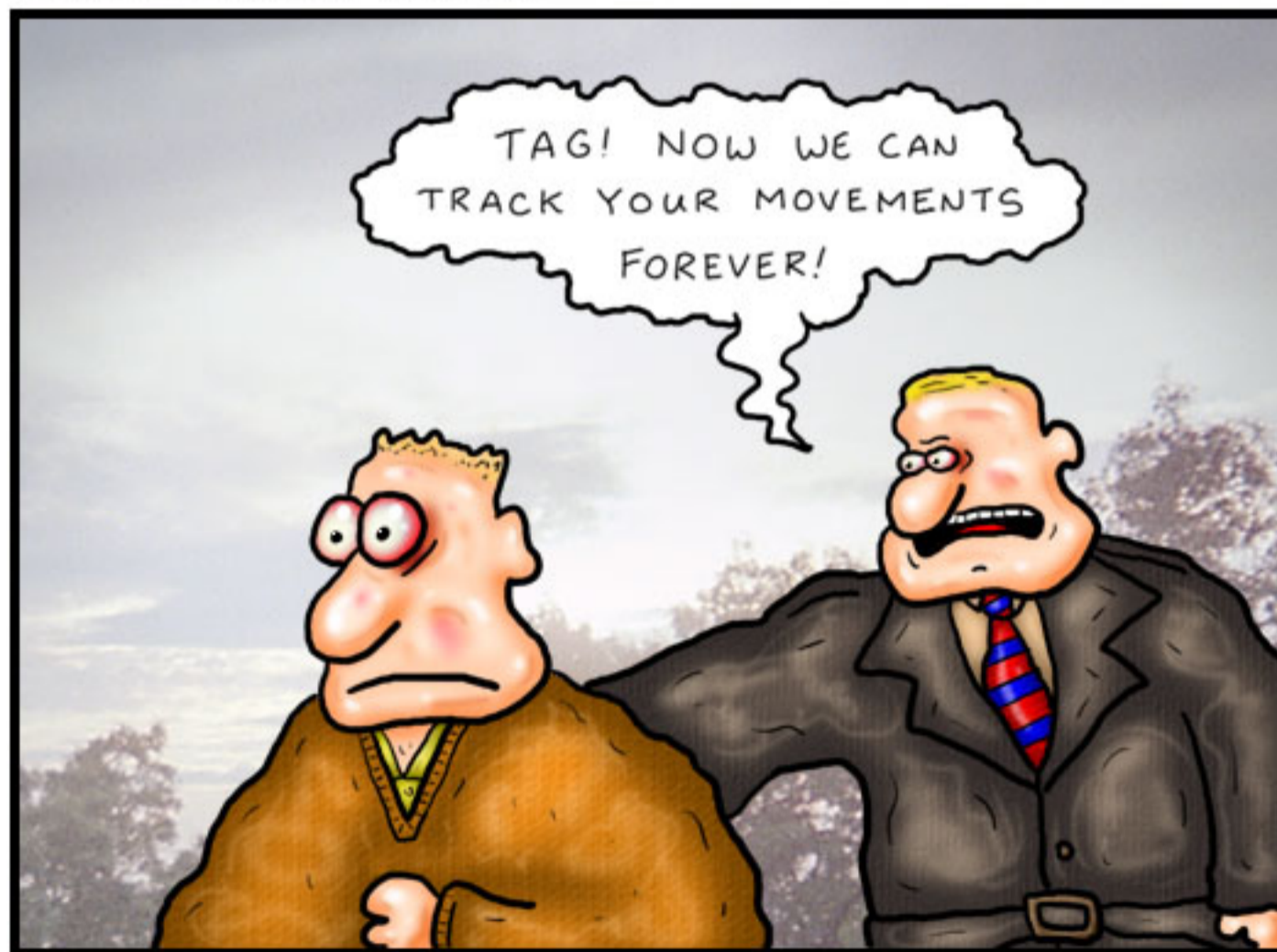
- The World Summit of Information Society has contracted SportAccess, a Company of Kudelski Group, as the main responsible of an integrated solution for physical access control solution during the United Nations Summit of Information Society. The MultiSAK system has already been deployed in other meetings as the World Economic Forum in previous years and was globally designed and developed by NagraCard and NagraID.
- The procedures of how personal data is being handled during WSIS break the principles of the Swiss Federal Law on Data Protection of June 1992 [2], the European Union Data Protection Directive 95/46/EC [3] and the United Nation guidelines concerning Computerized personal data files adopted by the General Assembly on December 1990.
- The Electronic Privacy Information Center [1] has an extensive news archive and background material on the subject of privacy threats and RFTags. Usage of RFTags in supermarkets, to tag products for purposes of stock management and security, has already attracted oppositions on privacy grounds by CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) [5] and has lead to campaigns for customer boycott of tagged products [6].

## REFERENCES

- [1] Electronic Privacy Information Center Website about RFID Identification <http://www.epic.org/privacy/rfid/>  
[2] Swiss Federal Law on Data Protection, <http://www.edsb.ch/e/gesetz/schweiz/index.htm>  
[3] European Union Data Protection Directive, [http://europa.eu.int/comm/internal\\_market/privacy/index\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/index_en.htm)  
[4] Guidelines for the Regulation of Computerized Personal Data Files, <http://www.unhchr.ch/html/menu3/b/71.htm>  
[5] - <http://www.nocards.org/AutoID/overview.shtml>  
[6]The Boycott Gillette Campaign - <http://www.boycottgillette.org/>

## DOCTOR FUN

8 Dec 2003



Copyright © 2003 David Farley, d-farley@ibiblio.org  
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

The new fun game of RFID tag

## RELATED NEWS

News in the following languages: Spanish, English, French, Dutch, German, Portuguese, Catalan, Galego...

- 2003-12-10 [SP] [WSIS hackeado](#)
- 2003-12-10 [GA, PT] [O WSIS foi hackeado!!](#)
- 2003-12-10 [SP] [El WSIS ha sido hackeado!!](#)
- 2003-12-11 [SP] [Burlada la seguridad de la Cumbre Mundial de la Sociedad de la Información](#)
- 2003-12-11 [EN] [What summit security?](#)
- 2003-12-12 [EN] [WSIS Physical Security Craked - \*\*Slashdot\*\*](#)
- 2003-12-12 [EN] [WSIS Security system violates the data protection guidelines](#)
- 2003-12-12 [EN] [More info and pictures of the physical security at WSIS](#)
- 2003-12-12 [CAT] [Han hackejat la WSIS](#)
- 2003-12-12 [FR] [La sécurité du forum mondial sur la société de l'information aurait été piratée !](#)
- 2003-12-12 [SP] [Amenaza a la privacidad de los participantes](#)
- 2003-12-13 [NL] [Inbraak in toegangssysteem WSIS-conferentie](#)
- 2003-12-13 [SP] [Entrevista con Alberto Escudero-Pascual, investigador de seguridad de ordenadores del Instituto Politécnico de Estocolmo, Suecia y miembro fundador del portal telemático Nodo50. 3609 KB MP3 \(Red con Voz\)](#)
- 2003-12-13 [FR] [La sécurité de l'accès physique au SMSI](#)
- 2003-12-14 [EN] [MIT's Furd Log](#)
- 2003-12-14 [EN] [Officials secretly RFID'd at Internet Summit - \*\*Slashdot\*\*](#)
- 2003-12-14 [EN] [Bug devices track officials at summit - \*\*Washington Times\*\*](#)
- 2003-12-14 [EN] [Officials bugged at international summit](#)
- 2003-12-15 [EN] [Why did WSIS bug delegates? - \*\*The Feature\*\*](#)
- 2003-12-16 [IT] [WSIS, i delegati erano spiati](#)
- 2003-12-18 [EN] [Summit group confirms use of ID chip - \*\*Washington Times\*\*](#)
- 2003-12-23 [FR] [RFID: les badges du sommet de Genève avaient des effets seconds](#)

## More related articles

- [RFID: les badges du sommet de Genève avaient des effets seconds](#) AFNET. Association Francophone des Utilisateurs du net

## THE PERSONAL DATA COLLECTION AT WSIS VIOLATES THE SWISS, EU AND UN DATA PROTECTION GUIDELINES

Here we describe the process we followed to obtain a secure badge of one of the participants. A high resolution of the pictures is available [here](#)



Every participant to WSIS follows the signs to the registration desk. The participants were requested to carry the LETTER OF INVITATION that includes a REGISTRATION NUMBER and an IDENTITY CARD.



The participants stand in a queue and provide a REGISTRATION NUMBER. The REGISTRATION NUMBER is checked against a database. The participants show an ID Card and a picture is taken of them via a Webcam.

*In our case we "only" provided the name of an existing participant that we obtained from the WSIS website and show a plastic card (as a secure ID Card) that contains the name of the participant and our picture.*



While we asked about the WSIS PRIVACY POLICY concerning the collection of personal data and what the badge contained, we did even have time to picture all the cameras. No extra information was obtained upon our request



NOONE INFORMED us in advance about the procedure, that our picture was going to be stored in a DATABASE and the period of data retention. NOONE INFORMED us that the badge contained a SmartCard and a Radio Identification (RFID) built-in that could be triggered remotely without the cardholder noticing. The badge is printed out in less than one minute. The whole procedure takes around 3 minutes.

By this time we had a badge of one of the participants containing our own picture. We spent the following days



making an analysis of what the badge contained. The control system is composed of a Radio Reader and a terminal. The Radio Reader exchanges secure messages with the badge of the participants.



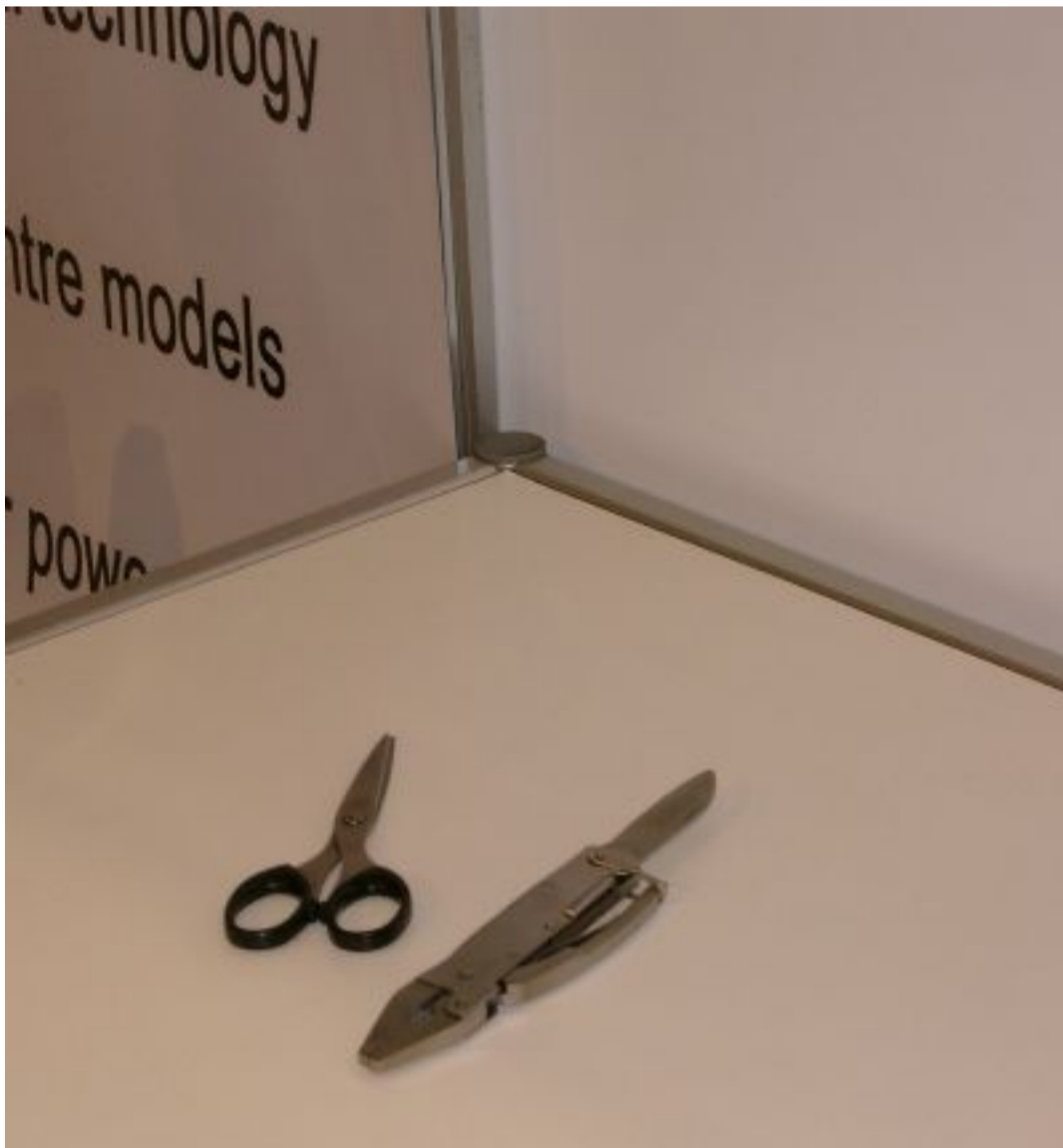
When a participant approaches a radio reader a set of transactions takes place in the centralized database. In the entrance, the associated picture to the name of the participant is retrieved. Other data of the participants is also retrieved as the name, affiliation and the times has entered the Congress. The system allows by datamining to obtain the human relationships of the participants.



Detail of one the proximity radio sensors. Sensor can be placed in the entrance of sessions rooms or a vending machine.



The system includes also a X-Ray and metal screening system. Two days before we were in the Congress bringing all kind of boxes and equipment. No physical access security was implemented until the very late time and we could move inside freely carrying any items.

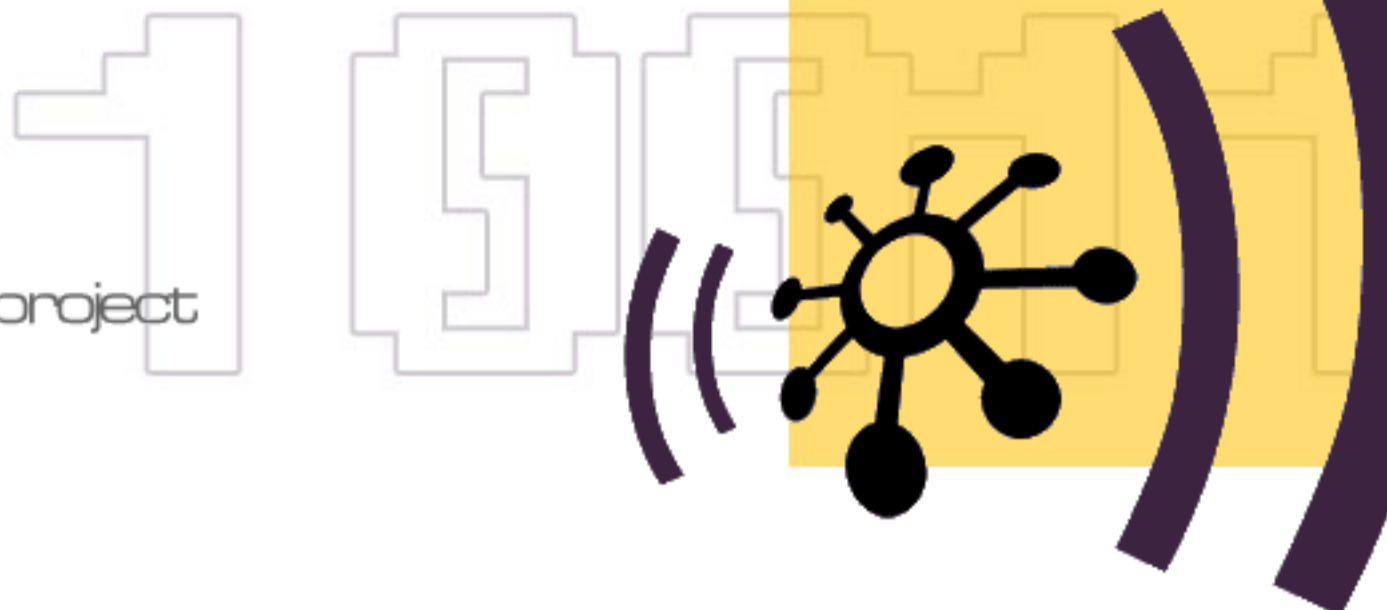


Days before the Summit no physical security was available. Anyone could bring anything inside the conference. We wonder if all the data collected about the participants is proportional and balanced. In the name of SECURITY the participants are pictured and screened, a huge database is created. What for? To protect whom?





1. This is the first time that the participant is aware what is carrying is not just a simple plastic card.
2. Upon request to the radio smart card, the picture and the rest of the personal data is requested from the database.
3. The picture in the badge, the picture in the terminal and the cardholder face are verified.
4. Physical Verification of the pictures is done by the Swiss Army dressed in uniform.
5. Data of the participants that entered the Congress just before is also visible in the screenshot. Notice that is possible to make pictures of the personal data.
6. A set of pictures of the people latest visitors is available. The system timestamps every entry.
7. A timestamp shows the last time that the participants entered the Congress.



[Subscribe](#) | [Contact Us](#) | [Proposals](#) |

[Publish](#)
[printable version](#) - [email this article](#)

- espanol -

### WSIS hackeado!

 by acp via (((i))) madiag *Wednesday December 10, 2003 at 11:48 PM*

Noticia reproducida de suburbia.

[http://suburbia.sindominio.net/breve.php3?id\\_breve=179](http://suburbia.sindominio.net/breve.php3?id_breve=179)

 El WSIS ha sido hackeado!!  
 Miércoles 10 diciembre 2003.

Un grupo de hackers ha sido capaz de entrar de manera no autorizada dentro del recinto donde se celebra la cumbre, demostrando y burlandose así del rudimentario sistema de seguridad que se esta empleando para el acceso controlado de los delegados y demás participantes e invitados.

El sistema está compuesto por una tarjeta plástica que contiene un chip capaz de transmitir el identificador personal así como el lugar en el que se encuentra el participante dentro del recinto, gracias a unos sensores de presencia que pueden estar colocados en cualquier parte: máquinas de refresco, salas de conferencias, entradas y salidas... de esta manera el sistema puede detectar donde se encuentra en cada momento cada persona, saber en qué sesiones ha participado, qué contactos ha realizado, con quien ha estado...

Este sistema no solo viola las leyes de protección de datos, ya que los asistentes no son informados de la existencia de esta base de datos ni de la posibilidad de almacenar y posteriormente tratar esta información sin su consentimiento.

Pero lo más interesante es que este avanzado de sistema de seguridad ha conseguido ser vulnerado y neutralizado, poniendo en cuestión además de su validez legal, su efectividad a la hora de controlar los accesos.

Pueden verse las fotografías del acceso por parte de los no-inscritos a la conferencia en la siguiente dirección web: <http://www.nodo50.org/wsispictures/>

Toda la información y los enlaces en inglés y gallego-portugués en esta noticia de la Casa Encantada en Indymedia Galiza: <http://galiza.indymedia.org/gz/2003/12/2234.shtml>

Nota en castellano modificada de Indymedia Madrid


[add your comments](#)


#### LATEST COMMENTS ABOUT THIS ARTICLE


Listed below are the 10 latest comments of 1 posted about this article. These comments are anonymously submitted by SF-IMC website visitors.


TITLE	AUTHOR	DATE
-------	--------	------

<a href="#">see original post on....</a>	circus	Wednesday December 10, 2003 at 11:43 PM
--	--------	---


 everything you want to know about Microsoft M12 10:15PM


 "Jail job" Oltre i co.co.co: le nuove frontiere dello sfruttamento M12 5:47PM


 ESF in London: a celebration for all and an invitation from few horizontals M12 3:36PM

 Call Center in sciopero M12 3:22PM

 IP Enforcement Directive Rushed through EU Parliament M12 1:16PM


 Bersagliata dal mobbing, Michela C. si ribella M10 1:15PM


 L'importanza di chiamarsi 'Open Source' M09 6:05PM


 EU IP Enforcement Directive Passed M09 3:45PM

 Laugh It Off in yet another copyright infringement battle M08 7:47PM

 MediaConnection#13 M06 9:19PM

 ANALYSIS: REPORT FROM THE THE WORLD SOCIAL FORUM. M06 3:02PM

 Mexico: Community Radio Stations Up Against The Wall M06 2:55PM

 US: IBM Settles Suit Over Toxic-Chemical Claims M06



## Artículos por Puntuación:

[Noticias mejor puntuadas](#)

[Análisis mejor puntuados](#)

[Convocatorias mejor puntuadas](#)

[Total mejor puntuadas](#)

## Artículos con multimedia:

[Video](#)

[Foto](#)

[Audio](#)

## Artículos por Tema:

[Desobediencia global](#)

[DOSSIERS indyACP](#)



Búsqueda

[Preguntas Frecuentes](#)

[Contáctanos](#)

La red Indymedia

Promedio: [8.50](#)

(nota media de [4 lectores](#) que han puntuado)

[¿De qué va esto de la puntuaciones?](#)

Página visitada **1988** veces

Wednesday 10 de December 2003, a las 17:37h.

[Enviar por mail esta historia](#)

[Imprimir historia](#)

## El WSIS ha sido hackeado!!

Por anónimo

**N**oticia publicada hace unos minutos por el HackLab de la [Casa Encantada](#), que participa en el proyecto "WSIS? We Size!" , contracumbre a la conferencia intergubernamental de la sociedad de la información haciendo públicos detalles del sistema de seguridad y las razones por las que este sistema atenta contra las leyes europeas de protección de datos!!

Traducción rápida del gallego-portugués:

El sistema está compuesto por una tarjeta plástica que contiene un chip capaz de transmitir el identificador personal así como el lugar en el que se encuentra el participante dentro del recinto, gracias a unos sensores de presencia que pueden estar colocados en cualquier parte: máquinas de refresco, salas de conferencias, entradas y salidas... de esta manera el sistema puede detectar donde se encuentra en cada momento cada persona, saber en qué sesiones ha participado, qué contactos ha realizado, con quien ha estado...

Este sistema no solo viola las leyes de protección de datos, ya que los asistentes no son informados de la existencia de esta base de datos ni de la posibilidad de almacenar y posteriormente tratar esta información sin su consentimiento.

Pero lo más interesante es que este avanzado de sistema de seguridad ha conseguido ser vulnerado y neutralizado, poniendo en cuestión además de su validez legal, su efectividad a la hora de controlar los accesos.

Toda la información y los enlaces en inglés y gallego-portugués en [esta noticia](#) de la Casa Encantada

[Nunca Más!](#)



[nodo50.org/wsisis](http://nodo50.org/wsisis)

En este monitor es donde el personal uniformado realiza la comprobación de identidad a la entrada del sistema.

[1] [2]

< [Una pequeña crónica acerca de cuatro días demasiado intensos](#) | [Aznar anuncia la detención de los presuntos asesinos de los agentes del CNI](#) >

¿Te gustaría puntuar esta historia? Pues [entra](#) y apúntate en la [Comunidad IndyACP](#) o, si solo tienes curiosidad, [puedes informarte de qué va esto](#) de las puntuaciones.

[www.indymedia.org](http://www.indymedia.org)**Proyectos**[oceania](#)[print](#)[radio](#)[satellite tv](#)[video](#)**África**[ambazonia](#)[nigeria](#)[sudáfrica](#)**Canadá**[alberta](#)[hamilton](#)[maritimes](#)[montreal](#)[ontario](#)[ottawa](#)[quebec](#)[thunder bay](#)[vancouver](#)[victoria](#)[windsor](#)**Lejano Oriente**[japón](#)**Europa**[andorra](#)[atenas](#)[austria](#)[barcelona](#)[bélgica](#)[belgrado](#)[bristol](#)[chipre](#)[estrecho / madiag](#)[euskal herria](#)[galiza](#)[alemania](#)[hungria](#)[irlanda](#)[istanbul](#)[italia](#)[liege](#)[lille](#)[madrid](#)[nantes](#)[países bajos](#)[niza](#)[noruega](#)[parís](#)[polonia](#)[portugal](#)[praga](#)[rusia](#)[suecia](#)[suiza](#)[salónica](#)[reino unido](#)[west vlaanderen](#)**América Latina**[argentina](#)[bolivia](#)[brasil](#)[chiapas](#)

Umbral:

**Qué interesante noticia** (Puntuación: 0)por anónimo el Wednesday 10 de December 2003, a las 20:52h. CET ([#1](#))

Esta noticia me ha interesado ya que muestra el grado de desarrollo de la tecnología para controlar a la gente y cómo nuestros amos están dispuestos a usar este poder contra nosotros, así como algunos recursos que aún tenemos para resistir.

He usado la palabra "amos" de acuerdo con el valor que le da el comisionado de la ONU Jean Zieler en su libro "Los nuevos amos del mundo", libro que aprovecho para recomendar.

Un lector.

[ [Responde a esto](#) | [Padre](#) ]**En inglés** (Puntuación: 0)por anónimo el Wednesday 10 de December 2003, a las 22:11h. CET ([#2](#))

La noticia y las fotos en inglés:

<http://www.nodo50.org/wsis/>[ [Responde a esto](#) | [Padre](#) ]**hay comunicado de prensa de los tres hackers** (Puntuación: 1, Interesante)por anónimo el Wednesday 10 de December 2003, a las 22:16h. CET ([#3](#))

los tres hackers que desarrollaron la acción han emitido un comunicado de prensa

[http://www.nodo50.org/wsis/WSIS\\_privacy\\_esp\\_draft0.2.pdf](http://www.nodo50.org/wsis/WSIS_privacy_esp_draft0.2.pdf) y además han convocado una rueda de prensa. ....se les puede escribir a [wsis@nodo50.org](mailto:wsis@nodo50.org) o [wsisi@conta.info](mailto:wsisi@conta.info) que es la misma dirección[ [Responde a esto](#) | [Padre](#) ]

- [Re:hay comunicado de prensa de los tres hackers](#) por anónimo el Wednesday 10 de December 2003, a las 22:34h. CET

**Fantástico** (Puntuación: 0)por anónimo el Thursday 11 de December 2003, a las 19:03h. CET ([#5](#))

Qué guapo!!! los malos jakeados :-)

Gracias a esa gente por hacerlo y a todos los que lo estáis difundiendo (Nodo50, Indymedia Galizia, etc.). Me ha encantado.

[ [Responde a esto](#) | [Padre](#) ]



## LINKS

- Summit Home
- Summit About
- Summit Contact
- Summit Disclaimer

.....

## COMPETITION

## YOU ARE HERE

[Home](#) | [Summit Life](#) |  
[What summit security?](#)

## SUMMIT ARCHIVE

- Developing World
- Digital Divide
- Education
- Environment
- Freedom of Expression
- Freedom of Information
- Gender
- Human Rights
- Information Society
- Infrastructure
- Intellectual property
- Internet Governance
- Media
- Protest
- Software
- Africa
- Asia-Pacific
- Europe
- Latin America
- Middle East
- South Asia
- Switzerland
- UK
- US
- Civil Society
- NGOs
- Private Sector
- United Nations

## [NEWS AND VIEWS]

« [Competition!](#) | [Home](#) | [Be afraid. Be very afraid.](#) »

December 11, 2003

**What summit security?** Activists have managed to obtain an official pass for the summit using an assumed identity and a fake plastic identity card - breaching the summit's supposedly tight security.

They are also furious that summit passes, which contain a radio chip, can be used to track the movements of delegates, with information stored in a central database - especially as the database could be transferred to the Tunisian authorities, who host WSIS 2 in 2005.

"The big problem is that system also fails to guarantee the promised high levels of security while introducing the possibility of constant surveillance of the representatives of civil society, many of whom are critical of certain governments and regimes.

"Sharing this data with any third party would be putting civil society participants at risk, but this threat is made concrete in the context of WSIS by considering the potential impact of sharing the data collected with the Tunisian government in charge of organizing the event in 2005."

David Steven @ December 11, 2003 12:34 PM | [TrackBack](#)

### Comments (0)

### Post a comment

Name:

Email Address:

URL:

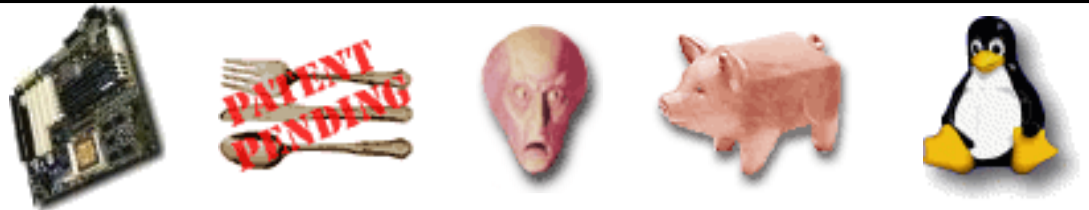
Remember personal info?

Yes No

Comments:

## RECENT COMMENTS

- Ask the Iranian Government. - (64)
- The Arabic take. - (1)
- AIDS in Nigeria: - (9)
- Iranian censorship? - (291)
- Mugabe tightens net. - (5)
- Competition! - (36)
- Free goodies. - (1)
- Saddam Hussein. - (28)
- So what do we know about John Marburger, - (3)
- Back to blogging. - (2)



**Login**

[Why Login?](#)  
[Why Subscribe?](#)

- Sections**
- [Main](#)
  - [Apache](#)
  - [Apple](#)
  - 1 more**
  - [Askslashdot](#)
  - [Books](#)
  - [BSD](#)
  - [Developers](#)
  - [Games](#)
  - 7 more**
  - [Interviews](#)
  - [Science](#)
  - 1 more**
  - [YRO](#)

- Help**
- [FAQ](#)
  - [Bugs](#)

- Stories**
- [Old Stories](#)
  - [Old Polls](#)
  - [Topics](#)
  - [Hall of Fame](#)
  - [Submit Story](#)

- About**
- [Supporters](#)
  - [Code](#)
  - [Awards](#)

- Services**
- [Broadband](#)
  - [Online Books](#)
  - [Personals](#)
  - [PriceGrabber](#)
  - [Product News](#)
  - [Tech Jobs](#)

**WSIS Physical Security Cracked**

Posted by [CowboyNeal](#) on Thu Dec 11, '03 10:56 PM  
from the [watching-the-watchmen](#) dept.  
An anonymous reader writes "A group of activists has apparently [bypassed physical security checks at the WSIS Meetings](#). Not only did they bypass the physical security with a fake card, they found the system uses [RFID tags](#) to monitor participants -- possibly even who they interact with and their movements through the conference."



**Unsurpassed speed**  
**6.0/768**

**Unrivaled price**  
**\$99.<sup>95</sup>/mo.**

[Click Here](#)

**Slashdot Login**

Nickname:

Password:

[\[ Create a new account \]](#)

**Related Links**

- [Dev Tools DevChannel](#)
- [Compare the best prices on: Software/Utilities](#)
- [bypassed physical security](#)
- [WSIS Meetings](#)
- [RFID tags](#)
- [More Security stories](#)
- [Also by CowboyNeal](#)

< [Linguistics Meets Linux: A Review of Morphix-NLP](#) | [Heads-Up Displays for Motorcyclists](#) >

[WSIS Physical Security Cracked](#) | [Log in/Create an Account](#) | [Top](#) | **196** comments | [Search Discussion](#)

Threshold:

**The Fine Print:** The following comments are owned by whoever posted them. We are not responsible for them in any way.

**Feels good** (Score:5, Funny)  
by [Hi\\_2k \(567317\)](#) on Thursday December 11, @10:58PM ([#7697617](#))  
(Last Journal: [Sunday November 16, @05:37PM](#))

These people are looking to be put in charge of my Packets, yet they cant even keep a couple of geeks out of a confrence room? I'm sure we'll all feel REALLY safe ordering online with them in charge.

**Re:Feels good** (Score:2)  
by [KrispyKringle \(672903\)](#) on Thursday December 11, @11:05PM ([#7697674](#))  
(<http://www.radioactivechicken.org/>)

So what's the point? I don't get it at all. You trust a loan officer with your financial information, but you don't expect him to be an expert in good eating.

What the ``activists" did was present a fake ID. Whoop de freakin' do. Certainly something stupid on part of the summit organizers, but not exactly failing to ``keep a couple of geeks out of a conference room."

The part I really don't get, though, is the fuss about the RFID tags. Guess what? I bet they were using them for the same thing that supermarkets and department stores use them for--electronic identification. If the ID cards had bar codes, would they complain that the bar codes are being used to electronically ID the holders? Sure, they can be read remotely, and that would bother me if they were given to ordinary consumers (say, like in *Minority Report*, when Cruise walks into a store and is greeted by name by a sales display). But at a conference you volunteer to attend to, run by a trusted organization (in theory, at least) with far less motive to engage in remote tracking and profiling than a major retailer, I'd say it's just not a huge concern.

But maybe that's just me. It's still an interesting article.

**Re:Feels good** (Score:5, Interesting)

by [cduffy \(652\)](#) <[cduffy+slashdot.spamcop@net](mailto:cduffy+slashdot.spamcop@net)> on Thursday December 11, @11:44PM (#7697892)

It's a security conference. There's a reasonable expectation is that security experts:

1. Are innately concerned about avoiding unnecessary exposure of personal data (say, by displaying it in such a way that 3rd parties could observe or record personal information about other attendants).
2. Will be able to use access control which is not circumvented by such a blatantly trivial mechanism as a fake ID.
3. Will not permit other physical security measures (such as the use of metal sensors) to be trivially circumvented (as by smuggling in items which would not be permitted to be taken in during the conference itself beforehand).

And so forth. The issue is not necessarily so much that the organizers are hostile as that they're incompetant in the very matter they're holding a conference about.

**RTFA** (Score:5, Informative)

by [lurker412 \(706164\)](#) on Friday December 12, @12:48AM (#7698218)

The World Summit on the Information Society is not a security conference. It is concerned with much broader issues of society and technology. You can find more info [here](#) [itu.int]

**Re:RTFA** (Score:2)

by [cduffy \(652\)](#) <[cduffy+slashdot.spamcop@net](mailto:cduffy+slashdot.spamcop@net)> on Friday December 12, @03:15AM (#7698769)

Pardon. I did indeed read the article, but my eyes somehow read "Information Security".

That said, I would argue that privacy and security are key among such issues, and would hope that those involved in such a society would be knowledgeable regarding it.

**Re:RTFA** (Score:2)

by [cduffy \(652\)](#) <[cduffy+slashdot.spamcop@net](mailto:cduffy+slashdot.spamcop@net)> on Friday December 12, @05:44AM (#7699192)

*The only thing these 'activists' are trying to do is give RFID tags a bad wrap.*

No, they also pointed out issues completely unrelated to the badges -- such as displaying members' information in such a way that others could observe or record it, easy circumvention of the metal detectors, and the like.

*The security badges they scammed are no different than the ones we've all been wearing to get into our day jobs for the past 10 years.*

The badge I wear to get into my day job is passive -- needs an EM field from the reader to do anything at all -- and readable only at a range tantamount to actual contact.

**Re:RTFA** (Score:3, Insightful)

by [John Harrison \(223649\)](#) on Friday December 12, @08:28AM (#7699830)

(<http://www.angelfire...nirak/tutorial/day6/> | Last Journal: [Monday August 18, @05:45PM](#))

I would guess that the badges are standard Mifare badges and can be read from a distance of about 5 cm at most. This is not something that is useful for passive tracking. You would have to knowingly present your badge to a reader. Funny how the article didn't mention that.

There are a variety of smart card and RFID standards, and the two are different animals. This "press release" did nothing to clarify what the cards were. If these guys were such amazing hackers we would know if it is a tag or a card and what the make and model are. We would know what was stored on the card and what security was in place on it. Instead we know just about nothing.

This could have been really interesting, but the press release is short on information and long on FUD.

**Re:Feels good** (Score:1, Interesting)

by Anonymous Coward on Friday December 12, @12:53AM (#7698245)

very believable at MobiComm this year the host hotel's wireless cisco routers were open for non authenticated access through telnet...

one would have thought that the net admin would have been a little worried when you're network is going to be used by a conference on mobile computing

**Re:Feels good** (Score:1)

by [utlemming \(654269\)](#) <[gro.gnimmeltu](mailto:gro.gnimmeltu@www) (ta) (www)> on Friday December 12, @08:51AM (#7699978)

(<http://www.utlemming.org/>)

They are experts in theory AND politicians. Further, they used contractors to implement the security. So for the most part, they were there to hash out a political agenda, not to actually worry about what they were talking about. In politics, people rarely care about the actual implementations of the goings-ons in a meeting, as long as they get to be heard. Unlike a Linux conference, security perse is not as important. If it was a Linux conference every geek would be looking over the security and judging it.

**Re:Feels good** (Score:1)

by [vtweb \(132332\)](#) on Friday December 12, @08:22AM (#7699776)

(<http://www.vtweb.com>)

The point in the article was the lack of notification to attendees of the data collection. In addition, no privacy policy was provided when requested.

**Re:Feels good** (Score:5, Insightful)

by [DataPath \(1111\)](#) on Thursday December 11, @11:20PM (#7697767)

It's even better than that.

The security at the conference is weak, and they're collecting personal data while they navigate the conference.

I think they've pretty much proven they're the wrong people for the job.

**Re:Feels good** (Score:4, Funny)

by [Geek of Tech \(678002\)](#) <[joshuarogers@hopper.net](mailto:joshuarogers@hopper.net)> on Thursday December 11, @11:30PM (#7697821)

(<http://www.hopper.net/~joshuarogers> | Last Journal: [Friday November 28, @09:26PM](#))

But don't worry about the data they collect! They're probably using 2-bit encryption! It's the only thing you can use with their 2-bit security measures.....

**don't underestimate 2-bit encryption** (Score:2)

by [SHEENmaster \(581283\)](#) <[su.borf](mailto:su.borf@retsamneehs) [ta] [retsamneehs]> on Friday December 12, @06:54AM (#7699398)

(<http://frob.us/> | Last Journal: [Friday December 27, @04:50AM](#))

If you guess wrong, you have to guess again! And if you get it wrong again, you must guess a third time! If you guess a fourth time without repeating guesses, you're in of course, but we're hoping no one will notice.

**huh?** (Score:4, Funny)

by [junkymailbox \(731309\)](#) \* on Thursday December 11, @11:01PM (#7697646)



Ok, so these guys "cracked" the system by finding the name of a person, got a fake id, went there, took a picture and walked in.

sidenote: all them kids in the clubs must be great crackers .. I see them "cracked" and "bypassed physical security" all the time ..

oh wait .. this is slashdot .. no one goes to clubs here ..

then they dissect the card that were given to them to find out that they have RFID chips but no one seems to know what it does. .. Wait .. how's this different than any other place that asks for your information .. like [Police and Lawyers Love EZPass](#) [slashdot.org]?

**Re:huh?** (Score:3, Interesting)

by [Cumstien \(637803\)](#) on Thursday December 11, @11:15PM ([#7697737](#))

From a forensic science conference I learned that law enforcement will use supermarket discount cards to place individuals at a particular place and time. You'd better think twice about saving \$.79 before whacking an adversary.

**Re:huh?** (Score:5, Funny)

by [segfault7375 \(135849\)](#) on Thursday December 11, @11:38PM ([#7697865](#))

(<http://www.draconianmist.net/>)

Yeah, but I bet you would feel differently about it if you were proven innocent because you were buying hand lotion and copy of Maxim when the crime was being committed.

**Re:huh?** (Score:2, Funny)

by [Trigun \(685027\)](#) <[janitor AT evilempire DOT ath DOT cx](mailto:janitor AT evilempire DOT ath DOT cx)> on Thursday December 11, @11:42PM ([#7697884](#))

(<http://evilempire.ath.cx/>)

In that case, I've been proven innocent in about a million crimes already! I love technology!

And Maxim...

**Re:huh?** (Score:2)

by [ATMAvatar \(648864\)](#) on Friday December 12, @12:07AM ([#7698001](#))

(Last Journal: [Sunday September 28, @11:48AM](#))

Not really. If I were buying hand lotion and Maxim, there would be witnesses to corroborate my story (the people in line and the person at the register). Not to mention, if you used a credit/debit card in that purchase, there would be a log of the transaction occurring and where it happened.

**Re:huh?** (Score:4, Funny)

by [HeghmoH \(13204\)](#) on Friday December 12, @07:57AM ([#7699638](#))

(<http://www.mikeash.com/>)

I'd rather go to jail for a crime I didn't commit than have a thousand strangers know that I read Maxim.

**Re:huh?** (Score:2)

by [kchayer \(161217\)](#) <[keith@cAAAhayer.net](mailto:keith@cAAAhayer.net) minus threewowels> on Friday December 12, @03:44PM ([#7705046](#))

(<http://www.chayer.net/>)

*I'd rather go to jail for a crime I didn't commit than have a thousand strangers know that I read Maxim.*

But you just admitted that very thing to a thousand strangers. :)

</tongue-in-cheek>

**Re:huh?** (Score:1)

by [fenix down \(206580\)](#) on Friday December 12, @12:42PM ([#7702714](#))

And that's why we have "beyond a reasonable doubt".

**Re:huh?** (Score:1, Funny)

by Anonymous Coward on Thursday December 11, @11:53PM ([#7697942](#))

That's why my VONS card is under the name Jeffery Lebowski

**Re:huh?** (Score:2, Interesting)

by [ParadoxDruid \(602583\)](#) \* on Friday December 12, @12:43AM ([#7698184](#))

(<http://www.paradoxdruid.com/>)

This is exactly why my friends and I have started a policy of trading Grocery cards with anyone new that we meet, and encouraging them to do likewise.

You get the same discount, you get to have some fun trading cards around and stuff, and they can't track you nearly as easily.

**Re:huh?** (Score:2)

by [anagama \(611277\)](#) <[thepotter@yaCOUGARhoo.com](mailto:thepotter@yaCOUGARhoo.com) minus cat> on Friday December 12, @04:20AM (#7698916)

I do this too! There should be a website to host such an exchange program - send in a [somestore] card, a SASE, and get a random [somestore] card back (same kind as you send in of course).

**Re:huh?** (Score:1)

by [Spyder \(15137\)](#) on Friday December 12, @12:08PM (#7702279)

1. Open phone book
2. Get some shmucks name and address
3. Use the shmucks info for your gorcery discount card
4. ????
5. Profit!

Just one more disconnect between the reliablity of authentication vs. identification. Not a novel or interesting hack, but the problem is so pervasive in these half-assed security systems that is almost always works.

Quote from George MacDonald's Flynn:

"The problem is, when you reduce people to little pieces of paper, somebody is going to give you the piece of paper and not the person." -- Flynn aka NN 13

(Might be a little off, I'm going from memory, and I haven't read the book in a few years)

**Re:huh?** (Score:1)

by [michaeltoe \(651785\)](#) <[michaeltoe@@@sailormoon...com](mailto:michaeltoe@@@sailormoon...com)> on Thursday December 11, @11:17PM (#7697747)  
(<http://michaeltoe.deviantart.com/> | Last Journal: [Tuesday September 09, @05:05PM](#))

The problem is that this is not a night club. It isn't different, it's stupid, and it's a big fat birthday invitation for potential abuse.

None of this would be a problem if the people making these decisions were in any way whatsoever educated in computer science. They're not, however, and considering their complete and utter incompetence regarding everything else they do... why should their involvement here be any better?

**Re:huh?** (Score:5, Insightful)

by [sholden \(12227\)](#) on Thursday December 11, @11:20PM (#7697766)  
(<http://sam.holden.id.au/>)

You can't see the difference between this and a club?

One is a venue which wants to transfer money from your wallet to them in exchange for alcohol and a good time. The government says they aren't allowed to take money from people below a certain age, so they don't let them in. If you have a fake ID, then why would the club care that you choose to spend your money on their product?

One is a venue filled with the heads of governments of numerous countries, government ministers, UN bigwigs (like the Secretary-General), and other such VIPs (in some people's eyes). It doesn't want to sell people a product which the government has decreed you have to be a certain age to have, but possibly wants to stop VIPs being harrassed and bombs being planted.

**Re:huh?** (Score:3, Interesting)

by [Geek of Tech \(678002\)](#) <[joshuarogers&hopper.net](mailto:joshuarogers&hopper.net)> on Thursday December 11, @11:34PM (#7697838)  
(<http://www.hopper.net/~joshuarogers> | Last Journal: [Friday November 28, @09:26PM](#))

>>> *Ok, so these guys "cracked" the system by finding the name of a person, got a fake id, went there, took a picture and walked in.*

Even worse. I think the article said "...a name from the WSIS website of attendees." No cracking, unless you consider surfing the web "cracking".

**Well. . .** (Score:5, Funny)by Anonymous Coward on Thursday December 11, @11:02PM ([#7697652](#))*Days before the Summit no physical security was available. Anyone could bring anything inside the conference*

Yep, it was fairly easy to sneak my tin foil hat in.

**so this is like 'hacking'** (Score:5, Funny)by Anonymous Coward on Thursday December 11, @11:04PM ([#7697669](#))

except they were walking around and stuff.... neat.

**Re:so this is like 'hacking'** (Score:2, Funny)by [Grey Tomorrow \(722221\)](#) on Friday December 12, @01:58AM ([#7698547](#))

I like to call it "warwalking". Catchy huh?

**Re:so this is like 'hacking'** (Score:1)by [dahamsta \(161956\)](#) <[slashdot@beecher.net](mailto:slashdot@beecher.net)> on Friday December 12, @07:15AM ([#7699473](#))[\(http://beecher.net/\)](http://beecher.net/)

This comment is much funnier than the parent. Who's in charge around here?

**"Bypassed security"** (Score:5, Insightful)by [JohnGrahamCumming \(684871\)](#) \* <[slashdot@jgc.org](mailto:slashdot@jgc.org)> on Thursday December 11, @11:05PM ([#7697675](#))[\(http://www.jgc.org/](http://www.jgc.org/) | Last Journal: [Friday August 22, @11:31AM](#))

Huh? If you RTFA you'll find that what they did was use a fake ID with the name of a real participant to obtain a badge. Nothing very clever about that.

Basically the "researchers" represented themselves as being someone else and used a fake (potentially) illegal piece of identification. Doesn't seem clever, just seems fraudulent.

They then go on to speculate about how "data mining" and RFID might be used for all sorts of nasty tricks and end up sounding like a bunch of paranoid crack-pots.

So, if I buy a fake passport on a street corner and then use it enter Germany, did I just "crack" Germany's security and can I get my picture on Slashdot?

John.

**Re:"Bypassed security"** (Score:5, Insightful)by [irokitt \(663593\)](#) on Thursday December 11, @11:13PM ([#7697729](#))

Nobody is saying the "crackers" were clever. We're saying the "Safety Experts" were stupid. They should have taken precautions in both the physical and electronic realms.

**Re:"Bypassed security"** (Score:3, Insightful)by [JohnGrahamCumming \(684871\)](#) \* <[slashdot@jgc.org](mailto:slashdot@jgc.org)> on Thursday December 11, @11:17PM ([#7697753](#))[\(http://www.jgc.org/](http://www.jgc.org/) | Last Journal: [Friday August 22, @11:31AM](#))

&gt; We're saying the "Safety Experts" were stupid. They should have taken precautions in both the physical and electronic realms.

So to fix the problem that the "researchers" exposed you need a participant to submit `_prior_` to the conference some token that only they would know or have. So they could have demanded a photo, fingerprint, eye scan, urine sample before hand. Then they could have demanded the same when getting your badge.

But you have to ask whether that would be an appropriate level of security for this event, and that comes down to assessing the level of threat.

Rather than being "stupid" I suspect that the security people didn't believe that such a high level of identification was necessary. They seemed to have used the same level that any US airport would use: show me a government issued ID and I'll accept it as genuine.

John.

**Re:"Bypassed security"** (Score:4, Insightful)by [Trigun \(685027\)](#) <[janitor AT evilempire DOT ath DOT cx](mailto:janitor AT evilempire DOT ath DOT cx)> on Thursday December 11, @11:45PM ([#7697903](#))[\(http://evilempire.ath.cx/\)](http://evilempire.ath.cx/)

Or they could have just sent out invitations by registered mail. If you wanted to get fancy, you could put the RFID in the invite, or \*gasp\* number them!

**Re:"Bypassed security"** (Score:2)

by [sholden \(12227\)](#) on Thursday December 11, @11:26PM (#7697800)

(<http://sam.holden.id.au/>)

*So, if I buy a fake passport on a street corner and then use it enter Germany, did I just "crack" Germany's security*

Obviously.

And it would be of great concern to Germany. Just as this should be of great concern to the organisers of the summit.

The probably don't want protesters or terrorists getting in just as much as Germany doesn't want illegal immigrants or terrorists getting through its security.

**Re:"Bypassed security"** (Score:3, Interesting)

by [dark404 \(714846\)](#) on Thursday December 11, @11:30PM (#7697819)

I think the pseudo-slang term you are looking for to describe what they did is, "Social Engineering." Unfortunately, the weakest link in any system of security (real or virtual) is the user. A parallel can easily be drawn from what was done here to the old days of AOL (maybe the current days too, been years since I used AOL) where script kiddies and wanabe hackers would 'phish' (compromise) accounts by impersonating AOL employees and asking people for their passwords over Instant Messages. Of course people FELL for that even with "AOL will NEVER ask for your password" plastered on every IM box on the system.

We should be able to trust our fellow man, and on many levels we want to trust people. Because of our predisposition to trusting people (when meeting them face to face, obviously on the internet it is a tad different) the unscrupulous take advantage of that trust. On one hand we're too trusting and get taken advantage of, on the other hand we're too untrusting and our society becomes overly unfriendly. Rock and a hard place.

**Re:"Bypassed security"** (Score:5, Insightful)

by [DataPath \(1111\)](#) on Thursday December 11, @11:31PM (#7697824)

I don't think the purpose of the writeup is to give m4d pr0pz to the 133t m34tsp4c3 haxxorz. It seems to me that the points they were trying to get across were:

- 1) These people have little concern for security, seeing as how they didn't even comply with the multiple applicable laws governing that sort of conference
- 2) These people have little concern for privacy, again, as they didn't comply with multiple applicable laws on the matter
- 3) Their ineptitude could possibly be opening these people for extortion or blackmail, or even endangering their lives.
- 4) These are the people who are deciding how the internet is going to be governed

**U.N. and the Internet** (Score:3, Insightful)

by [TWX \(665546\)](#) on Friday December 12, @12:34AM (#7698132)

(<http://www.blacksatin.net/>)

*"4) These are the people who are deciding how the internet is going to be governed"*

Not to get too off-topic, but I don't think that I like the direction that they want to take the Internet. Yes, it spans the globe, but it's something that a lot of private and public American funding went into designing, developing, and maintaining. I understand the need for standards, but I don't think that the U.N. is really right for governing the Internet. They have a hard enough time running peacekeeping missions in *European* countries, let alone anywhere else in the world, and that's stuff that there has been established methods around for quite some time.

My basic idea is this-- The U.S. had the single largest contribution to the idea of a global information network in the form of the Internet. If the rest of the world wants one of their own, let them create it themselves. There are enough people in enough other countries that if they want to slowly combine into one government with it's own infrastructure, let them. It's called *competition*, and it's been proven, that when coupled with the right amount of cooperation, to be very good at advancing things. If the U.N. builds their own global information network and it's better than the Internet, people will switch. If it's not, either through information availability problems, or through censorship, then it won't. Seems fairly simple.

**Re:U.N. and the Internet** (Score:2)

by [DataPath \(1111\)](#) on Friday December 12, @12:45AM (#7698200)

I agree. There aren't many organizations that would be a poorer choice for governing the internet, but if I understand correctly, that is EXACTLY what WSIS is intended to be doing.

**Re:U.N. and the Internet** (Score:1)by [You're All Wrong \(573825\)](#) on Friday December 12, @03:12AM (#7698761)

"It's called competition, and it's been proven, that when coupled with the right amount of cooperation, to be very good at advancing things."

The giraffe and the crab are a product of competition.

They consider themselves the most advanced long-necked-thing and walks-sideways-thing in the world.

Want an IT example? The browser with the blink tag was more advanced than the browser that came before it.

YAW.

**Re:U.N. and the Internet** (Score:2, Insightful)by [Stachel \(718095\)](#) on Friday December 12, @06:55AM (#7699399)

*They [the UN] have a hard enough time running peacekeeping missions in European countries*

The UN might be more capable/powerful running those missions if the U.S. were paying their share of the contribution.

*The U.S. had the single largest contribution to the idea of a global information network in the form of the Internet. If the rest of the world wants one of their own, let them create it themselves.*

Ha, but a European guy invented HTML, without which 'American' internet would be pretty useless, wouldn't it?

--

Stachel

**Re:U.N. and the Internet** (Score:2)by [DataPath \(1111\)](#) on Friday December 12, @09:19AM (#7700182)

having used the internet quite a lot before the "invention" of HTML, I find your statement uninformed. We had a world wide web before the world wide web - it was called gopher. It didn't have graphics or blink tags, or even a choice of fonts, but darnit! We liked it anyway! IIRC it had something resembling hyperlinks, which with or without this "a European guy" (I've never heard the story of the invention of HTML), would have evolved just like everything else on the internet.

Oh yeah - what made the internet useful when I was a kid. Usenet, of course - you have user communities and support forums on the web - that was all on Usenet. ftp - downloading games and a few shareware productivity programs that made windows 2.0 just a little bit nicer. e-mail, not that I at that age had anyone to email, but it was there. And those are just the things that my little 9 year old self had contact with, there were all kinds of unix utilities that used the internet (or networks of one sort or another) to do useful, productive things.

**Re:U.N. and the Internet** (Score:1, Flamebait)by [j-b0y \(449975\)](#) on Friday December 12, @07:41AM (#7699579)

I think that the U.N. as an entire organization gets a bad rap due to the going-nowhere and doing-nothing nature of the General Assembly (a talking shop, par excellence) and the Security Council (almost always veto-deadlocked, and impotent even when it does agree on something). However, the ITU, along with other organisations under the U.N. umbrella (like the UNHCR), doesn't actually do a bad job as such.

If it wasn't for some obtuse decisions and the opaque decision-making process which ICANN has specialised in, and the commercialisation of the Internet at a core level (Hi VeriSign!); I doubt very much if anyone would care who ran the Internet. Unfortunately, the running of the Internet does have the look of an elite club about it (for good historical reasons), and those on the outside feel disenfranchised by the process through which decisions are made for them.

In the end, this isn't about who's better at running the Internet, but rather a case of who has the power.

**Re:"Bypassed security"** (Score:2)by [DataPath \(1111\)](#) on Friday December 12, @09:29AM (#7700264)

From the article:

The procedures of how personal data is being handled during WSIS break the principles of the Swiss Federal Law on Data Protection of June 1992 [2], the European Union Data Protection Directive 95/46/EC [3] and the United Nation guidelines concerning Computerized personal data files adopted by the General Assembly on December 1990.

They said "how the data is being handled", they didn't elaborate more, and I'm not qualified to speculate on the legality of anything. My objective was more to restate rather than reinforce the original article.

**Re: "Bypassed security"** (Score:2)

by [jmv \(93421\)](#) <[valj01.gel@usherb@ca](mailto:valj01.gel@usherb@ca)> on Thursday December 11, @11:31PM ([#7697825](#))  
(<http://www.xiph.org/~jm>)

Well, they still proved that the security system was pretty much useless because the weakest link was somewhere else (only a simple ID with no other info is sufficient). It's like saying "my front door lock is unbreakable" and leaving the back door open. And BTW, I believe it's still harder to get a fake passport with your picture on it than to do what they did.

**Re: "Bypassed security"** (Score:5, Interesting)

by [ShaunC \(203807\)](#) on Thursday December 11, @11:37PM ([#7697852](#))  
(<mailto:s@shat.mypants.net>)

If you RTFA you'll find that what they did was use a fake ID with the name of a real participant to obtain a badge. Nothing very clever about that.

You'll also find that they should have been required to produce their letter of invitation and a registration number. They had neither, but got in anyway. Perhaps not so much clever as scary, this place is hopping with "important people" and anybody can walk right in with no invite and a fake ID.

The security at freaking MacWorld was better (or worse, depending on your perspective) than this the last time I went! Unless you got your badge via mail, you had to produce not only your ID but also the credit card that you used to register. Not infallible, but at least a challenge - and Javits wasn't full of diplomats, either.

**Re: "Bypassed security"** (Score:3, Funny)

by [whereiswaldo \(459052\)](#) on Friday December 12, @12:08AM ([#7698006](#))  
(Last Journal: [Friday October 17, @10:04PM](#))

*So, if I buy a fake passport on a street corner and then use it enter Germany, did I just "crack" Germany's security and can I get my picture on Slashdot?*

Give it a try. I think that's how David Hasselhoff got his big break.

**Re: "Bypassed security"** (Score:2)

by [GQuon \(643387\)](#) on Friday December 12, @12:20AM ([#7698052](#))  
(<http://www.bowlingfortruth.com/> | Last Journal: [Monday December 08, @06:30AM](#))

*can I get my picture on Slashdot?*

No. That could only happen in three ways:

- Paying for an ad.
- Hacking slashdot.
- Being so obnoxious that you get your own topic icon. Like Bill Gates.

**Re: "Bypassed security"** (Score:2)

by [ScrewMaster \(602015\)](#) on Friday December 12, @12:42AM ([#7698181](#))

*... and can I get my picture on Slashdot?*

No, but I'm sure it would appear on a few mug shots.

**Re: "Bypassed security"** (Score:2)

by [penguin7of9 \(697383\)](#) on Friday December 12, @12:49AM ([#7698224](#))

*So, if I buy a fake passport on a street corner and then use it enter Germany, did I just "crack" Germany's security*

Yes.

*and can I get my picture on Slashdot?*

No, because there is no particular expectation that German security is any better than that of, say, France or the US. European nations don't have a lot of security along their borders with other Western nations. So, it isn't hard for an American to enter Germany, France, or the UK illegally.

However, there is a natural expectation that security experts have better security at their own conferences than the annual conference of, say, Flower Arrangers of America.

**Re: "Bypassed security"** (Score:1)

by [LynXmaN \(4317\)](#) \* on Friday December 12, @05:22AM (#7699121)

(<http://www.lynxman.net/>)

Well and I've bypassed American border controls after September 11th with my Spanish passport, and the best thing is that I even didn't want to, they just made me bypass it because there was no contact telephone at my entering visa... and I still keep it since nobody wanted it back, they just told me to keep going.

So... no country or no place is secure when there is a human that have the final decision to overpass the system at his own will ;)

**Might have been an inside job** (Score:2)

by [John Harrison \(223649\)](#) on Friday December 12, @09:00AM (#7700038)

(<http://www.angelfire...nirak/tutorial/day6/> | Last Journal: [Monday August 18, @05:45PM](#))

caption from one of their photos:

*The system includes also a X-Ray and metal screening system. Two days before we were in the Congress bringing all kind of boxes and equipment. No physical access security was implemented until the very late time and we could move inside freely carrying any items.*

Why were they bringing in equipment two days before? Were they testing security or were they employed to carry stuff around by the conference? If the latter is true then it isn't much of an accomplishment to have gotten in.

Also in one of the photos of the "ominous security screen" the name is clearly "John DOE". Why is this the case? No explanation is given. This whole writeup is poorly done. They also offer no proof that they actually got in. Just some pictures of the security area. They don't even have a high-resolution shot of the card itself.

So what exactly does this article prove? That /. will post any crap that makes RFID look bad. That's about it. It isn't even clear if they are using RFID as opposed to say ISO14443 cards.

**easy solution** (Score:3, Funny)

by [markov\\_chain \(202465\)](#) on Thursday December 11, @11:07PM (#7697686)

microwave for 1s

**No Seriously...** (Score:2)

by [TubeSteak \(669689\)](#) on Friday December 12, @04:32AM (#7698947)

(Last Journal: [Friday August 22, @01:31AM](#))

would this work?

[google seems to think so](#) [google.com] The truth of the matter is that a microwave oven is massively over-powered for the job of killing RFID tags

**Re:No Seriously...** (Score:1)

by [idiosync \(130620\)](#) on Friday December 12, @04:27PM (#7705618)

(<http://avantgarde.8m.com/cl/>)

Just wait until microwave ovens are illegal in the US under the DMCA.

**Further proof (as if any was needed)** (Score:4, Funny)

by Anonymous Coward on Thursday December 11, @11:10PM (#7697705)

that geeks are merely terrorists under another name!

**Tracking locations?** (Score:4, Interesting)

by [fred911 \(83970\)](#) on Thursday December 11, @11:10PM (#7697711)

In order to track locations to see who's close to who, you need many, many rfid transceivers. Probably so many, so close there'd be other issues (rf issues).

**Re:Tracking locations?** (Score:3, Interesting)

by [interiot \(50685\)](#) on Friday December 12, @12:41AM ([#7698170](#))  
(<http://paperlined.org/>)

Read the article, the badges are "passive" in that they only reflect radio waves sent to it. Also, the RF transmitters/sensors are placed only at entrances and pop machines, so attendees weren't tracked really closely, and apparently they can't sense much more than 20 feet away, making RF interference much less of a problem.

**Nothing is safe.** (Score:5, Insightful)

by [irokitt \(663593\)](#) on Thursday December 11, @11:11PM ([#7697713](#))

The fact that the security was breached is not the most alarming thing about this. Nothing programmed by man is ever completely safe. The scary thing is that people professing to be security concious were bested because of something so simple, and which could have been prevented or easily stopped.

**Re:Nothing is safe.** (Score:1)

by [slazar \(527381\)](#) on Friday December 12, @12:47PM ([#7702770](#))

As opposed to something programmed by god? :P

**Still Important** (Score:4, Insightful)

by [digitalvengeance \(722523\)](#) on Thursday December 11, @11:16PM ([#7697744](#))

Though many have criticized this article as not really representing cracking or bypassing security in any impressive manner, I think there is a deeper issue here.

What information of use could be gleaned at future meetings or other UN events? The same people very likely do event security for this and other conferences, and the type of information that could be gleaned or the damage that could be done at other events is something to be taken seriously.

Personally, I despise the UN - but they (through US) are a force in the world and a breach of their security is nothing to laugh at too quickly.

**Historical parallel..** (Score:5, Insightful)

by [irokitt \(663593\)](#) on Thursday December 11, @11:18PM ([#7697759](#))

The problem here was one of physical security-all these guys really needed to get started was a name. During the 80's/early 90's, one of the concerns in the security field was also physical security-a hacker posing as a janitor and accessing unsecured systems, or dumpster diving, or using personal connections to get at employees and talk something valuable out of them. I would think that people would have learned by now that it takes more than simple electronic measures to stop "hacking". This could have been prevented if the powers-that-are had made the ID process a little harder.

**[RFID] Late night on slashdot and the nightmare...** (Score:5, Insightful)

by [the man with the pla \(710711\)](#) on Thursday December 11, @11:20PM ([#7697764](#))

begins.

They are going to put these in tires. When you buy your tires the seller is going to be required to enter your information in a database.

One day when you are going a little too fast in a school zone or run a yellow that switches to red too fast an underground computer is going to sense the rfid in your tire, immediately reporting the number via rf link to police headquarters.

You would think that this would be for the purpose of giving you a ticket. You're right, you will get a ticket. But that is not the end the trail for your rfid number.

It immediately gets sent to the state government where it checks to make sure you are not a deadbeat dad that the wherabouts of are unknown. Simultaneously sending it to the FBI to see if you are a name on the "patriot" act watchlist and indexes your location. If you drive on the same street on a regular basis they will know where to find you.

You're not a deadbeatdad, lawbreaker, or terrorist you say??? Well the trail that your rfid number takes does not end there. Your rfid number is sold by cashed-strapped states to a commercial database under the auspices of "risk mitigation" that insurance companies subscribe to. Because you were speeding, you are at an increased risk and your car insurance rates are subsequently raised. Because you drive dangerously, your health insurance rates are also raised. Maybe they cancel your policy outright.

You're thinking I'll just remove the rfid. No you won't. Driving with unregistered tires is against the law, and if the police can't scan you as you drive past his cruiser he pulls you over and immediately suspends your license and



impounds your car. But you won't be able to remove it anyway, without destroying the tire, as it is purposefully integrated with the "steel belt".

Does the trail end for your rfid tire number now? No, it most certainly doesn't. To see where it leads further, you are going to have to talk to my patent attorney.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1, Informative)  
by Anonymous Coward on Thursday December 11, @11:43PM ([#7697890](#))

What is it that makes you think RFID technology suddenly enables this?

Lemme clue you in, there's this wild and crazy technology that puts a unique identifier on every automobile driving on public roads. It's linked to your name in state databases and it's required by LAW. It's called a license plate, you dumb shit.

And amazingly, if you get caught by an officer speeding in a school zone or blowing a red light, they will run your license plate in their little laptop to see if you have any warrants out, like for being a deadbeat dad.

And your car insurance company has the ability to look up your driving record to see any tickets or accidents within the past few years.

I'd assume that most anyone has this ability, an assumption based on the fact that if you get a speeding ticket, within 2 days you'll receive about 150,000 postcards in the mail from ticket attorneys and driving schools.

Get a clue you dumb piece of shit.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:2, Informative)  
by [Grue \(3391\)](#) \* on Friday December 12, @02:32AM ([#7698667](#))  
(<http://www.itsdarkhere.com/~josh/>)

RFID technology automates all this, no need for the cop anymore. No need for visually checking license plates. Suddenly everyone and anyone is tracked.

That is the big difference. The fact that this information will be entered into several hundred databases automatically.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1)  
by [Slayer \(6656\)](#) on Friday December 12, @03:54AM ([#7698862](#))

AFAIK there exist cameras which automatically pick up license plate information. Here in Austria it's used for section control, where they place two such cameras at a given distance and automatically issue a ticket if you need too little time to cover the distance.

Point is: RFID serves interesting purposes but certainly not that of surveying ordinary citizens. One good purpose might well be intercepting car thieves at the border. Remember. it's simple to swap license plates, whereas it takes time and effort to swap all four tires without getting noticed.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1)  
by [Seahawk \(70898\)](#) <[tts@ij.le.dk](mailto:tts@ij.le.dk) [['mag' in gap](#)]> on Friday December 12, @04:25AM ([#7698928](#))  
(<http://www.csworld.dk/>)

The difference is that a RFID reader is much cheaper than a videocamara + a system that enables it to actually read a dirty license plate.

And since it is cheaper, it will be more easy to setup more places.

And why stop at tires - what if(when?) it gets integrated in clothes?

(Not that I think it will happen where I live - just trying to make a point!)

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1)  
by [Slayer \(6656\)](#) on Friday December 12, @11:08AM ([#7701474](#))

When it came to surveiling and oppressing their own people, money was never an issue even for the poorest countries in the world. Laws against unreadable license plates exist in at least every country which issues automated speeding tickets through radar boxes.

Integrating RFID in clothes won't work. Cars are strongly regulated - people are used to the fact that they have to ask their government for kind permission to operate a car. If you put restrictions on clothes, even the dumbest soap opera watching pop corn munchers will start an outcry.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:3, Informative)  
 by [narratorDan \(137402\)](#) <[narrator@earthlink.net](mailto:narrator@earthlink.net)> on Friday December 12, @01:23AM ([#7698397](#))  
<http://home.earthlink.net/~narrator/>)

Simple way of taking care of the RFID tags in this tin hat situation;

Pay cash, (until the gov stops printing it, they must accept it) give them a fake name and phone number (the phone book is full of them), buy or make a RFID reader and locate the tag in the tire and cut that section of the tire out and put it in a microwave for about 30 seconds. DING! The RFID tag is fried, now replace the cutout in the tire and freely run down kids in school crosswalks with the red lights.

Hmm, just read the rest of your post. You're screwed.

NarratorDan

**Re:[RFID] Late night on slashdot and the nightmare** (Score:2)  
 by [RzUpAnmsCwrds \(262647\)](#) on Friday December 12, @01:46AM ([#7698492](#))

"Pay cash"

What if they put RFID in the cash?

**Re:[RFID] Late night on slashdot and the nightmare** (Score:3, Interesting)  
 by [narratorDan \(137402\)](#) <[narrator@earthlink.net](mailto:narrator@earthlink.net)> on Friday December 12, @02:42AM ([#7698691](#))  
<http://home.earthlink.net/~narrator/>)

They could, but cash changes hands so quickly it would be a lesson in futility. The better idea would be to ban cash (cash is too easy for terrorists to counterfeit) and go solely with credit/debit cards which *do* have RFID tags as part of the smart chip.

NarratorDan

**Counterfeit - cash or card?** (Score:2)  
 by [moncyb \(456490\)](#) on Friday December 12, @04:14AM ([#7698902](#))  
 (Last Journal: [Sunday November 23, @12:19PM](#))

CASH too easy to counterfeit??? As a certified terroristcriminal(TM), I'd rather work with the credit/debit cards. Smart chips are fun to hack. Anyway, CC companies don't care about fraud, they just push the costs onto the merchant. ;-)

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1)  
 by [ToadSprocket \(628571\)](#) on Friday December 12, @12:52PM ([#7702831](#))

\*Gasp\* You mean, with an RFID tag in my credit card, the collective evil "they" will know exactly when and where I use it, only mere moments afterward?

**Re:[RFID] Late night on slashdot and the nightmare** (Score:2)  
 by [fuzzybunny \(112938\)](#) on Friday December 12, @03:37AM ([#7698820](#))  
 (Last Journal: [Friday December 12, @07:21AM](#))

-Hotels.

-Flights.

-Rental Cars.

-Anything via the Internet or phone.

Good luck with the cash, dude. I like the sentiment, I agree with it, but realistically?

**Re:[RFID] Late night on slashdot and the nightmare** (Score:2)  
 by [YrWrstNtmr \(564987\)](#) on Friday December 12, @09:26PM ([#7708068](#))

*Pay cash,*

And the tire guy merely records your car license plate and/or VIN in the transaction. Same result.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:3, Informative)  
 by [clickety6 \(141178\)](#) on Friday December 12, @07:50AM ([#7699610](#))

*Isn't the UK already thinking of taxing every car "seen" on key roads once a day, every day they show up?*

Noppe, not thinking of it - in the "congestion zone" of London they are already DOING this!

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1)  
by [DarkVader \(121278\)](#) on Friday December 12, @09:55AM (#7700513)

So, this is a bit offtopic, but a serious question about this system.

Why can't you just put an LCD shutter over your license plate, and trigger it when you pass the camera? They'd be unable to read the plate, and you would be effectively invisible to the tracking.

If you wanted to get really fancy, you could record the GPS positions of all the cameras, and automate the shutter.

It seems to me that as long as there wasn't a cop car behind you, it would be pretty close to zero risk.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:2)  
by [surprise\\_audit \(575743\)](#) on Friday December 12, @02:13AM (#7698609)

Four different tags, one for each tire? Or just one tagged tire? How long would it be before folks started holding swap-meets to exchange tires? Make that illegal too, I suppose.

But then, are you going to make illegal the large parking lots full of swappable tires outside, say, WalMart? Or any Mall? How long would it take to exchange 1 "hot" tire *without* the knowledge of the donor?

Why stop at tires anyway? A tag in the battery would be more difficult to remove, and look at all the power available for it to punch a signal out with when it gets pinged by the detector... Tag the oil filter, engine crankcase, transmission. All this would be done in the guise of tracking down thieves that steal cars and strip them for parts...

Forget tagging car parts, consider how much easier it would be to tag the people... No need to carry a forgeable ID, just let the officer ping your embedded tag. Think you don't have one? Remember that prostate exam, or the last flu shot, or that root canal, or other similar procedure? Hmmm...

I'm assuming I'm remembering correctly something I read recently about the tags only being about the size of a grain of rice. Obviously anything bigger would be difficult to implant without the implantee being aware.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:2)  
by [Loosewire \(628916\)](#) \* on Sunday December 14, @11:28AM (#7717096)  
(<http://www.loosewire.co.uk/> | Last Journal: [Wednesday November 19, @05:23PM](#))

they require an airtel so this makes them much bigger, still worrying....

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1)  
by [badboy\\_tw2002 \(524611\)](#) on Friday December 12, @05:18AM (#7699106)

Hi there! Here's the deal: A system you envision would require thousands of readers in a local area to even get just the major chokepoints in a moderate sized metropolitan area. This is going to require a dedicated group of workers to maintain these buggers (power, networking, and eventual breakage from exposure to the elements because unlike velcro the aliens didn't give the tech to us) That's a bunch of people. I'll tell you what: I go outside on MY street and I see a bunch of freaking potholes in the street. Traffic is congested all over the place, and nonstop construction doesn't keep pace with population growth in the area.

So you're telling me that the good people of the land are going to vote this system in? Ahead of say a new lane on the bottleneck highway or perhaps some new pavement so we don't all actually require H2s to navigate the streets?

Who's paying for this tinfoil technology? Not the state governments, that's for sure. You seem to forget that despite the wild slippery slope theories people come up with, no one really looks at the practicality of making such a system work. Embedding millions of RFID tags nation wide at the cost of billions and billions of dollars to build and operate just doesn't seem like something people want.

But don't worry, this is just FUD. I work for THEM, and now that you're onto us Mr. Slashdot #ID 710711, we're going to have to shut you up. After all, we know where you are! (Cue creepy music)

**You're not a deadbeatdad, lawbreaker, or terrorist** (Score:2)  
by [way2trivial \(601132\)](#) on Friday December 12, @08:56AM (#7700012)

Or a speeder..... what now?

How is this different than a ticket issued by a cop who's using radar, and by the way- the state I live in, and every one I have lived in- automatically does give moving violations to insurance agencies, and rates do rise! based on violations of the motor vehicle sort..

I've been having this ethical oddity lately.. from my youth when I was a rebellious sort, to now when I have wife child home, and don't believe in 'breaking the law'

I do feel strongly people are entitled to privacy and freedom of choice.. but the solution to the original post is Don't be a deadbeat, lawbreaker, terrorist, or speeder (interesting the OP doesn't consider speeders under lawbreaker)

**License plate** (Score:2)

by [ajlitt \(19055\)](#) on Friday December 12, @09:52AM ([#7700478](#))

(<http://www.csoft.net/~ajlitt>)

I hear that the DOT has developed a new driver identification system called 'license plate'. It uses a specially developed optical identification system that can be read at a distance not only by sensors but by individual motorists. The serial number encoded on each 'license plate' can be used with a government database to identify the owner of the vehicle and even reference their criminal record.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:1)

by [ToadSprocket \(628571\)](#) on Friday December 12, @12:56PM ([#7702898](#))

Why do the foil hatties come out in droves whenever the subject of RFID's comes up? If someone really cares about you so much that they want to track your every waking moment, they will. There is only so much usefulness in an RFID anyway. One ex-cop thrown off the force for drinking Thunderbird following you around all day will give you much more info than an RFID tag ever could. And you can pay him in grain alcohol.

**Re:[RFID] Late night on slashdot and the nightmare** (Score:2)

by [f0rt0r \(636600\)](#) on Saturday December 13, @02:26AM ([#7709216](#))

Of course, I purchased the tires and donated them to a poor(er) person who could not afford new tires on their own. Looks like I got busted for someone elses crimes. Damn, this will hold up in court for sure!

**Yawn** (Score:1, Insightful)

by Anonymous Coward on Thursday December 11, @11:26PM ([#7697799](#))

> they found the system uses RFID tags to monitor participants -- possibly even  
> who they interact with and their movements through the conference.

Or they could just use a camera to follow your movements through the conference and see who you interact with. Nothing new here... move along.

**What a load of bull** (Score:1, Insightful)

by Anonymous Coward on Thursday December 11, @11:27PM ([#7697805](#))

If anyone really wanted to track people by "remotely activating" their RFID tags without them knowing, they would need so many of these close-range readers that you wouldn't be able to walk! Plus you would need to figure out who's who by getting into the "DATABASE" that nobody knows about.

You might as well drop one of these nifty wireless camera in each corner of the room, betcha it would be way more effective for tracking people's whereabouts.

PS/ I hear they (Privacy Enemies) can track me down and see whatever I'm doing only by knowing my IP address!!!  
pH34r

**Convenience vs Security** (Score:3, Insightful)

by [pbug \(728232\)](#) on Thursday December 11, @11:27PM ([#7697807](#))

(<http://www.posterbug.com/>)

The problem with any system in place is that when convenience is place ahead of security. The more convenient it is made for the people who it is going to protect and the people who are enforcing the system the less secure it will become. Well at least that is what I think part of the problem is.

**Since when did /. report on physical security?** (Score:4, Insightful)

by [LostCluster \(625375\)](#) on Thursday December 11, @11:31PM ([#7697822](#))

(<http://www.studioqb.com/>)

This wasn't a technical hack by any means... they brought a fake ID with the name of a real person on the guest list, and they got that person's badge issued to them. From that point on, they had as much clearance as that real person had, not surprising at all.

Just goes to show the inherent insecurity in demanding only a government-issued ID when many governments are involved. Any given state's drivers license has many anti-forgery features, but unless you have an inch-thick book with all of the features of every acceptable ID listed, an international event is gonna have a hard time relying on that alone.

Still, what's newsworthy about this failure? It happened at an important-to-the-Internet event, but it didn't really cause and damage...

**...yet** (Score:1)

by [learza \(710720\)](#) on Thursday December 11, @11:53PM (#7697944)

Since when did /. exclusively report on computer security?

You're right, it wasn't a technical hack, but that doesn't mean it's not important. Social engineering (which I guess this comes under) deserves more respect than it currently gets. Your organisation might have God's own firewall but that's not a lot of use if an attacker attends a conference at your workplace, gets a temporary ID and then gets lifts a couple of laptops at lunch.

**Re:Since when did /. report on physical security?** (Score:2)

by [surprise\\_audit \(575743\)](#) on Friday December 12, @02:19AM (#7698626)

*From that point on, they had as much clearance as that real person had, not surprising at all.*

Was anything done to prevent the real person showing up? If the organisers had discovered that person's badge had already been issued, they should have cancelled its clearance and sent someone through the crowd with a scanner looking for the associated rfid tag.

**Mitnick should take advantage of this one** (Score:2, Insightful)

by [MagicBox \(576175\)](#) on Thursday December 11, @11:58PM (#7697965)

His biggest \*break-ins\* were physically walking into a computer room. Nowadays that is the least talked about security issue. Mitnick does a lot of educating on the topic but a lot of people called him \*old fashion\*. Well there you go, it happened, and to none other than WSIS. I think you should check those locks on your server rooms again.

**Re:Mitnick should take advantage of this one** (Score:1)

by [MagicBox \(576175\)](#) on Friday December 12, @10:25AM (#7700882)

*Mitnick has already taken advantage.. that's why he went to prison. WHY take advice from a loser that got caught?*

Is he a loser because he got caught, or because he did what he did? I wasn't suggesting he should take advantage by starting to hack again, I was suggesting he should take advantage of the situation to get the message out there.....a lot more people might be willing to listen

**Mr Delegate Do You See Why We Need To Crack Down!** (Score:2, Insightful)

by [Linus Sixpack \(709619\)](#) on Friday December 12, @12:16AM (#7698032)

(Last Journal: [Friday December 26, @10:41PM](#))

Group of idiots commit fraud to crash an important meeting and discover -- rf tags. Then in sanctimonious puffery they tell the world about it because...

Do you not think the organizers knew there were limits to what they had to spend on security?

Rfid tags have the advantage of not needing an interpreter if the delegate only speaks another tongue.

See who gets painted by the same brush as these jerks, not scientists, not researchers...

**New, unique technology** (Score:2)

by [djuedal \(584558\)](#) on Friday December 12, @12:28AM (#7698095)

...that allows people to be tracked by their looks, voice, smell, gait, handedness, hair color, height, skin color and sex.

It is possible to track interaction around a room or hall between individuals, while also recording conversations, gestures and purchases.

The collected data can be recalled at any time, based on any combination of queries or profiles.

What kind of technical gadget is this?

My memory. Be afraid....be bery, very afraid.

**Reminds me of Apple Stores** (Score:2)

by [TubeSteak \(669689\)](#) on Friday December 12, @04:02AM ([#7698879](#))

(Last Journal: [Friday August 22, @01:31AM](#))

[This article](#) [wired.com] came to mind because of the quote:

For example, Allen has discovered that Apple uses a sophisticated video-monitoring system to automatically count the number of customers who enter the store, and to document their behavior once inside.

According to Allen, Apple uses a [ShopperTrak](#) [rctanalytics.com] system to count the number of people passing the store, the percentage who enter, and the percentage of those who make a purchase. Allen declined to state his source. An Apple spokeswoman confirmed that the company carefully tracks consumer traffic and buying patterns, but wouldn't discuss its methodology.

Its not to hard to extend this type of technology to a large gov't bulding and integrate it with your rfid database of movements. I know its tinfoil hat material, but its not much of a stretch.

**RFID Tags sucks** (Score:1, Insightful)

by Anonymous Coward on Friday December 12, @12:56AM ([#7698255](#))

Why does everyone think RFID tags can be used to monitor the actions of people?

RFID tags are un-powered. In fact, they are powered by the RF signals that are used to read the RF tag. Because of this RF tags have transmission range of inches.

**Re:RFID Tags sucks** (Score:2)

by [surprise\\_audit \(575743\)](#) on Friday December 12, @02:26AM ([#7698644](#))

Wanna bet that a tag in any battery powered device would be limited to inches?

How far can a cellphone can reach out to hit a cell tower? A mile or two? A tag in the battery ought to be able to reach out many yards, at least. Similarly, a tag in a car battery ought to have a good range...

**More than just Physical Security Issues** (Score:4, Insightful)

by [MojoReisen \(218327\)](#) on Friday December 12, @02:00AM ([#7698553](#))

This is probably another case of "You get what you pay for", but the issues here go beyond simply using a fake ID to breach physical security. The fact that the data needed to fake the ID was culled from the attendee list on the website speaks volumes as to how much thought actually went into the security architecture for this event. I mean, really, someone should of thought of that possibility. Why didn't they verify or vet this identification in some way ? Another frightening fact is that these jokers' security processes, if you consider the RFIDs as 'security',are violating the laws of both the host country and the EU. This is the biggest issue, IMHO. "Security" also means adhering to all applicable laws and regulations, in order to limit your liability, and the liability of your employer. And what about these guys walking around snapping photos of the screener's monitors ? Whats up with that ? The bottom line is that these "security experts" at SportAccess, or wherever, are incompetent. Their security model was ill-conceived, poorly executed, needlessly intrusive and (obviously) completely ineffective.

**Re:More than just Physical Security Issues** (Score:4, Insightful)

by [nagora \(177841\)](#) on Friday December 12, @04:06AM ([#7698888](#))

*if you consider the RFIDs as 'security',are violating the laws of both the host country and the EU.*

I'm sorry but you seem to be confused: laws are for little people, not big, wise, important people that can be trusted like our leaders.

TWW

**So what about the person who was imitated?** (Score:3, Insightful)  
by [GodLogiK \(650517\)](#) on Friday December 12, @03:07AM (#7698753)

I'm curious what happened to the person who they pretended to be... were they sick? Just didn't show up? Or when they came did security say, "sorry sir you've already signed in" deemed him a fake and locked the real guy away and are torturing him even as we speak? I dunno curious about that....

**Re:So what about the person who was imitated?** (Score:1)  
by [moumine \(637104\)](#) on Sunday December 14, @04:01PM (#7719369)

The Hudson does not flow through Geneva dude, it is the Rhone that does

**Fake ID cards** (Score:3, Funny)  
by [Zog The Undeniable \(632031\)](#) on Friday December 12, @04:19AM (#7698912)

If this was the type of card you just flash at an underpaid, gum-chewing security guard, the authors of the article didn't have to go to much effort to produce a fake.

As part of physical security testing, my colleagues have successfully gained access to premises using

- a white sachet of tartare sauce
- a square-cut jam sandwich

It's difficult enough getting security guards to turn up for work on the minimum wage, let alone actually \*challenge\* people.

**Total BS - been there** (Score:3, Interesting)  
by [cocotoni \(594328\)](#) on Friday December 12, @04:29AM (#7698937)

The part about RFID tags used for tracking is utter and total BS. In fact yesterday I was at WSIS. I did have the badge, and yes it is marked with a RFID, but the bugger is passive and I had to put it real close to the scanner to read it. I tried to just casually swipe it from afar, but I had to actually put it right in front of the reader.

More on security: at the entrance you walk through metal detector gates, with a X-ray scanner for the bags. You are processed by 4 security guys - one takes your bags, other works the gate and X-ray scanner, third scans your badge and compares your face to picture on the badge to picture in the DB they get based on the RFID tag. All these images have to match. If there is any problem there is the fourth guy standing behind with a rifle.

Yes - the 1337 h4x0rz could have bypassed this by getting the official badges, because when you have the badge you don't have anything standing in your way. No - they could not have gotten to the bigwigs, because that part of the conference was separated, with stronger security checks, which were obviously not done just at the place, since the bigwigs were escorted from their mansions, with the whole entourage, and I suppose that you don't expect presidents and prime-ministers to go around carrying badges on the straps around their necks, and walk through the metal-detector gates a few times.

In fact, the easiest way for "terrorists" to sneak in would be to get listed as active participants by a friendly government of a rogue state.

I wish that people would concentrate more on the positive results of WSIS, instead of spreading FUD.

**Re:Total BS - been there** (Score:3, Insightful)  
by [HeghmoH \(13204\)](#) on Friday December 12, @08:02AM (#7699653)  
(<http://www.mikeash.com/>)

*I suppose that you don't expect presidents and prime-ministers to go around carrying badges on the straps around their necks, and walk through the metal-detector gates a few times.*

You know, if there was some kind of law that said all those powerful politicians have to wait in line and go through the security screenings just like us "little people", I bet airport security would be a lot better and more convenient than it is right now. I thought the President was a person, just like you and me. So if I have to wear a badge and go through a metal detector, I think He (whoops, I mean "he") should to.

Politicians making decisions that have no effect on themselves piss me off to no end.

**Re:Total BS - been there** (Score:2)  
by [HardCase \(14757\)](#) on Friday December 12, @10:19AM (#7700810)  
(<http://www.fluidlight.com/drew>)

Hey, don't blame the politicians...for the most part, they don't demand special treatment. It gets offered by their hosts. As an example, if you do any amount of travelling to Washington, DC, you may notice your representatives or senators up there in first class. Chances are pretty good that they didn't buy a first class ticket, but no airline offering first class seating is going to watch as a high ranking politician sits with the hoi polloi. They get upgraded as a "courtesy". Ditto with the standing in line business, although here in Idaho, everybody stands in the same line to get screened by security, whether you're me or the governor.

Given that the president has his own plane, I guess he isn't subject to the same security screening as the rest of us. For that matter, the reason that the heads of state tend to not have to go through the same screenings as you or I is because the security is there for their benefit.

And as far as politicians making decisions that have no effect on themselves goes, every decision that they make has an effect - make a good one, stay in office. Make a bad one, get voted out.

That being said, I do understand your frustration at endless lines of waiting because of security "requirements". But even if the bigwigs had to go through the lines, nothing would change. Part of the problem is the one size fits all approach to nationally mandated security requirements. What works for New York City doesn't fit the bill for Boise, Idaho.

-h-

**Re:Total BS - been there** (Score:2)

by [HeghmoH \(13204\)](#) on Friday December 12, @02:28PM ([#7704058](#))

(<http://www.mikeash.com/>)

I will happily blame the politicians. Even if they aren't the ones deciding to skip all of the security, they *are* the ones making all of the useless rules in the first place. And I don't think that they would be making such useless rules if they were also subjected to them, particularly since politicians travel by air more often than other people.

The problem isn't really one-size-fits-all requirements. The problem is that the people who decide these things have decided that making people *feel* safe is more important than making them *be* safe. There are a dozen freight-train sized holes in airport security today which any intelligent person can discover from simply flying a few times, and could exploit with little effort. Meanwhile, security guards are patting down grandmothers and confiscating miniature swiss-army knives. But since the people who make these rules never have to deal with the consequences, they have no incentive to get rid of the inconveniences that only make people feel safe, and replace them with things which are simultaneously more convenient and more secure. This is not an oxymoron; nearly *any* imaginable setup would be more secure than what we have today. The only thing today's security setup can really stop are crazies who try to bring a duffel bag full of AK-47's or dynamite onto the plane. It won't stop anybody with half a brain, and as we have seen, there are quite a few people who have half a brain and want to do harm.

**Re:Total BS - been there** (Score:1)

by [zaroastra \(676615\)](#) on Friday December 12, @08:26AM ([#7699818](#))

*I wish that people would concentrate more on the positive results of WSIS, instead of spreading FUD.*

I wish they would indeed.

Some interesting things there. Just today I was talking with Mr. Edgar Villanueva after a open source debate.

I saw several nice projects from underdeveloped countries.

I hope it will go beyond the good intentions.

Now security wise, it seems a little like fud. I had some problems getting an exhibitor badge (not even the picture/rfid enabled one), because i only had an id card and the guys where asking for passports.

In the end, the easiest way to compromise security would be bringing the "things" on the days preceding the exhibition, where no security checks where made. I carried boxes containing 15 computers. Of course none opened them to see if something was inside.

**Two comments** (Score:4, Informative)

by Anonymous Coward on Friday December 12, @05:23AM ([#7699125](#))



I'm a delegate to WSIS, so I've been here for going on three days...

First, the security here is quite interesting...as other posters have mentioned, getting into the actual facility is more or less impossible without the proper badge. The exploit that these individuals used was to simply trick the badging desk - a location right next door manned (mostly) by teenage girls. I highly doubt that they're trained security professionals.

Two, the RFID badge has a range of about an inch. If there are transponders all over the place, I have yet to see them. The physical layout of the building would make it difficult to place them inconspicuously...there's far too much open space, with thirty foot ceilings...

Just my two cents (CHF)...

**Security** (Score:5, Insightful)

by [salesgeek \(263995\)](#) on Friday December 12, @07:37AM (#7699570)

When I was in the US Navy, I got to learn a few things that most security experts get to learn the hard and embarrassing way:

- 1) Security is hard work and requires the involvement of people with great integrity willing to work very hard. Security requires the highest level of attention to detail, trust that procedures will be followed and absolute trust that when the procedures don't work, don't apply or are circumvented that the individual will make the right decisions.
- 2) You cannot delegate security to any machine. This includes padlocks, safes, computers, surveillance systems, and alarm systems. These are all designed to assist the hard working humans with great integrity. They have no ability to make decisions when their processes fail, are circumvented or don't apply.
- 3) The inclusion of anyone without great integrity inside a secured area is insecure. Loose lips sink ships. This is why security is so difficult in any semi-democratic organization - there is no way to exclude those you can't trust.
- 4) Confidence is like corrosion. It slowly destroys even the strongest security just as corrosion will eventually sink the most powerful ship in the fleet.

Sounds like WSIS violated three of four of these rules.

**Just more proof** (Score:1)

by [CaptainFrito \(599630\)](#) on Friday December 12, @08:00AM (#7699644)

that only an utter fool would throw away civil liberties for the [impossible] promise of enhanced "security" via technology. While it is clear this monitoring and surveillance is useful in harrasing the innocent citizenry just trying to get through their pressure-filled day, there is zero proof it does anything more. More anxiety, less actual security, higher taxes, more days in court, more fines. Perfect.

The inexperienced put faith in every word, the shrewd look to history as prologue.

**Re:Just more proof** (Score:1)

by [Hiigara \(649950\)](#) on Friday December 12, @08:58AM (#7700026)

Uhh... did you even read the article?

**Re:Just more proof** (Score:1)

by [CaptainFrito \(599630\)](#) on Friday December 12, @06:59PM (#7707164)

Uhh...yes I did. Here's the relevent excerpt for my comment:

"An international group of independent researchers attending the World Summit on the Information Society (WSIS) has *revealed important technical and legal flaws*, relating to data protection and privacy, in the security system used to control access to the UN Summit. *The system not only fails to guarantee the promised high levels of security but also introduces the very real possibility of constant surveillance of the representatives of the civil society.*" (Italics added.)

The so-called "security system" indeed used advanced technology, not for security but for surveillance of the innocent, violating the basic human right to presumption of innocence and 'the right to be left alone'. AS a security system it was useless, but then again it was obviously not meant to be one. Homeland Security. Patriot Act. Etc.

Umm, so, did YOU read the article?!?

**Better case is made by the "pictures" page** (Score:5, Informative)

by [Halo- \(175936\)](#) on Friday December 12, @09:42AM (#7700355)

(<http://slashdot.org/>)

I have to admit the main link was a bit of a let-down, but after following the link to the [pictures](#) [nodo50.org] page, I start see why this is a big deal. A few things happened which aren't well expressed in the main link:

1. Participants were sent credentials which were supposed to serve as a second form of ID. The activists circumvented this second ID by simply claiming to be someone else and showing a generic fake ID. The list of participants was available beforehand, which was a mistake. Think of it like if an airport published lists of all the passengers on a plane and allowed "ticketless" travel using any form of ID. (instead of government issued photo ID) You just need to say you're "John Smith" and present a fake *anything* (library card, etc...)
2. Notice all the cameras in the photos? That's sorta creepy. My bank doesn't have that many.
3. There are pictures of RFID scanners, which means the whole "they are gonna track participants movements" bit isn't entirely tinfoil-hat paranoia. The presence of the sensors implies they plan to track.
4. There were metal detectors and X-Ray machines maned by the Swiss Army (insert knife joke here) at the entrances, but they didn't get placed until very later. The "safety" this buys the participants is marginal unless the entire conference center was sweep very, very carefully after the gates were put up. Most people with the motive to blow up an international conference don't do it as a spur of the moment thing. When a head of state visits somewhere, an advance team sweeps the room/route/etc and seals it as they go.
5. Privacy and data security are totally lacking. The organizers failed to inform participants about what information was to be collected, and more severely, couldn't produce a detailed accounting when asked. The data collected was visible on monitors to casual observers, which completely negates most of the value and allows for theft.

In short, the photos show a group that appears to know how to spend a lot of money on toys, but doesn't know how to use them. I think this is a serious concern. The information they are collecting isn't providing security, and could actually undermine it.

The illusion of security is worse than no security at all.

**This little stunt proves nothing** (Score:2)

by [JonKatzIsAnIdiot \(303978\)](#) on Friday December 12, @10:22AM ([#7700845](#))

from the article:

*The World Summit of Information Society has contracted SportAccess, a Company of Kudelski Group, as the main responsible of an integrated solution for physical access control solution during the United Nations Summit of Information Society.*

This stunt proves nothing about the security and privacy practices of WSIS, despite the general clamour in this forum. This was a minor slip-up of a third party, not WSIS itself. SportAccess gave passes to people who misrepresented themselves.

BTW - what's up with the 'bypass physical security' euphemism? I always thought it was called 'sneaking', as in 'I snuck into a bar' or 'I snuck into a movie' and was done by underage punks who wanted to go where they had no business being. Now it's done by 'independant researchers' and it's 'bypassing physical security'? Hmmm ... maybe I'll do some 'independant research' of my own at the ROTK premiere next week ...

**RFID == increase of portable microwave emitters** (Score:1)

by [l8apex \(582898\)](#) on Friday December 12, @01:26PM ([#7703314](#))

y'know- for frying RFID tags embedded in things that won't fit in your microwave..

**Privacy & WSIS** (Score:1)

by [privaterra \(641535\)](#) on Saturday December 13, @08:21AM ([#7710031](#))

(<http://www.privaterra.org/>)

The issue is bigger than one of the the use of RFID's, but one of data handling practices and policies. Held in Geneva, it's a UN summit, but what if any data privacy and freedom of information policies exist at the UN - NONE. That that issue wasn't raised at all , by anyone, is the tragedy.

**Re:'Activist' is such a misnomer** (Score:5, Insightful)

by Anonymous Coward on Thursday December 11, @11:00PM ([#7697634](#))

activism P Pronunciation Key(kt-vzm)

n.

The use of direct, often confrontational action, such as a demonstration or strike, **\*\*in opposition to\*\*** or support of a cause

Nope, activist sounds right to me.

**Re:'Activist' is such a misnomer** (Score:5, Insightful)  
by [glpierce \(731733\)](#) on Thursday December 11, @11:01PM ([#7697638](#))  
(<http://glpierce.deviantart.com/>)

I believe the word you're looking for is *conservative*.

**Re:'Activist' is such a misnomer** (Score:5, Interesting)  
by [Orne \(144925\)](#) on Thursday December 11, @11:46PM ([#7697907](#))  
(<http://www.geocities.com/polysillycon>)

No, Reactionary is one tick stronger on the scale

*Political Leaning* - "Left" to "Right"

Revolutionary - Liberal - Status Quo - Conservative - Reactionary

*Government Intervention* - "Weak" to "Strong"

Anarchist - Libertarian - Status Quo - Authoritarian

**Re:'Activist' is such a misnomer** (Score:1)  
by [utlemming \(654269\)](#) <[gro.gnimmeltu](mailto:gro.gnimmeltu@ta.www) (ta) (www)> on Friday December 12, @08:46AM ([#7699958](#))  
(<http://www.utlemming.org/>)

Reactionary carries such a strong meaning -- it is the direct opposite of a radical. A reactionary is one that reacts violently, or vehemently to ANY change from traditional values or ideas. By definition, a reactionary is above a conservative. The ranking goes from Conservative to Ultraconservative to Reactionary. A reactionary make Rush Limball look mild.

**Re:'Activist' is such a misnomer** (Score:3, Insightful)  
by [iminplaya \(723125\)](#) on Thursday December 11, @11:01PM ([#7697642](#))

I kind of interpret "activist" to mean that they are ...uhh..."active"? whether they are opposing or otherwise.

**Re:'Activist' is such a misnomer** (Score:1)  
by [michaeltoe \(651785\)](#) <[michaeltoe@@@sailormoon...com](mailto:michaeltoe@@@sailormoon...com)> on Thursday December 11, @11:10PM ([#7697708](#))  
(<http://michaeltoe.deviantart.com/> | Last Journal: [Tuesday September 09, @05:05PM](#))

Change can be good, and it can also be stupid...

Like Forest Gump, only with political clout.

**Re:'Activist' is such a misnomer** (Score:5, Interesting)  
by [anagama \(611277\)](#) <[thepotter@yaCOUGARhoo.com](mailto:thepotter@yaCOUGARhoo.com) minus cat> on Thursday December 11, @11:15PM ([#7697740](#))

What's this WSIS about? It seems you sneer at activists when in fact, they might just be protecting your freedom.

*It doesn't help that there are several topics of great import but huge controversy. The chief among these is Internet governance. In short: who gets to run the Internet?*

\*\*\*

*The United States, Europe and English-speaking partners such as Australia favour the existing private-company organisation, ICANN. Whereas developing nations, China, India, Brazil, South Africa and others all want a recognised international body to run the show, ITU.*

[Follow the links back a bit.](#) [theregister.co.uk]

And for posters below who seem unimpressed that a quasi governmental agency can monitor who it is you mingle with, or go to private areas for private discussion - you deserve what you'll get. The internet so far has been a model of a borderless world. But many countries are terrified by this concept - you really want them collecting data, manipulating who the attendees will be to prevent certain individuals from blocking their plans? That's nuts.

**Re: WTF** (Score:2)

by [KrispyKringle \(672903\)](#) on Thursday December 11, @11:17PM ([#7697746](#))  
(<http://www.radioactivechicken.org/>)

*Or am I just crazy and paranoid because of what's happening to my country right now (USA)?*

Yes.

*Is it too much to ask that the folks "in charge" let a true people's democracy develop without being waylaid and corrupted by corporate and special interests?*

Well, got a history book? I'd say yes to this, as well.

**Re: WTF** (Score:2)

by [bhima \(46039\)](#) on Friday December 12, @01:49AM ([#7698508](#))

Yeah, He's way too late wanting a true people's democracy in the US. His grand parents sold him out for giant cars with fins, colour TVs and cheap consumer goods made by 3rd world slave labour.

**Re: 'Activist' is such a misnomer** (Score:2)

by [JonKatzIsAnIdiot \(303978\)](#) on Friday December 12, @10:05AM ([#7700647](#))

You're right. An 'activist' is someone who screams very loudly about something they know nothing about. Gun control activists whose knowledge of firearms is limited to what they see on TV. Anti-GM food protesters without a working knowlege of genetics. Hordes of anti-globalization weenies who can't explain what globalization is, much less why they're against it, and really only came to the march to hang out with their friends.

**Troll** (Score:1)

by [GoneGaryT \(637267\)](#) on Friday December 12, @02:16PM ([#7703924](#))

(Last Journal: [Friday December 19, @04:56PM](#))

Dear Mr/Mrs/Miss/Ms/Dr/Prof/etc Moderator, please recognize the above post by prisoner 303978 Idiot as a troll.

Thank you.

**Re: 'Activist' is such a misnomer** (Score:2)

by [JonKatzIsAnIdiot \(303978\)](#) on Friday December 12, @04:04PM ([#7705318](#))

And what's more - they don't take criticism very well.

(see above)

This discussion has been archived. No new comments can be posted.

*Whip it, whip it good!*

All trademarks and copyrights on this page are owned by their respective owners. Comments are owned by the Poster. The Rest © 1997-2004 [OSDN](#).

[ | | | | | | | | | ]

# German Civil Society at WSIS

« [Civil Society started Free Wireless Network](#) | [Main](#) | [security system on wsis violates data protection guidelines](#) »

December 10, 2003

## PRESS CONFERENCE: WSIS: High privacy threat for the Civil Society

World Summit on Information Society: The personal data collection practises in the summit is a threat for the privacy of the participants. It´s on friday, 11.30h at the [geneva presse club](#)".

PRESS CONFERENCE, RUEDA DE PRENSA.

GENEVA PRESSE CLUB - CLUB SUISSE DE LA PRESSE

Friday 12th December 2003 at 11.30 am

à « La Pastorale », Route de Ferney 106 à Genève

[http://www.pressclub.ch/menu/sub\\_menu/adresse\\_csp.html](http://www.pressclub.ch/menu/sub_menu/adresse_csp.html)

GENEVA, 10th DEC 2003

An international group of independent researchers attending the World Summit on the Information Society (WSIS) has revealed important technical and legal flaws, relating to data protection and privacy, in the security system used to control access to the UN Summit. The system not only fails to guarantee the promised high levels of security but also introduces the very real possibility of constant surveillance of the representatives of the civil society.

During the course of our investigation we were able to register for the Summit and obtain an official pass by "just" showing a fake plastic identity card and being photographed (via a webcam), with no other document or registration number required to obtain the pass. The limited personal data required to produce the fake ID and thus register was easily obtained - a name from the WSIS website of attendees.

However this is only half of the story.

The official Summit badges, which are plastic and the size of a credit card, hide a "RF smart card" [1] - a hidden chip that can communicate its information via radio frequency. It carries both a unique identifier associated with the participant, and a radio frequency tag (RFID) that can be "read" when close to a sensor. These sensors can be located anywhere, from vending machines to the entrance of a specific meeting room allowing the remote identification and tracking of participants, or groups of participants, attending the event.

The data relating to the card holder (personal details, access authorization, account information, photograph etc.) is not stored on the smart card itself, but instead managed by a centralized relational database. This solution enables the centralized system to monitor closely every movement of the participants at the entrance of the conference center, or using data mining techniques, the human interaction of the participants and their relationship. The system can potentially be extended to track

participants' movements within the summit and detect their presence at particular session.

Because all of the personal data is stored in a centralized database, any part of the database can be replicated locally, or transferred to future events - for example the next WSIS Summit hosted by the Tunisian authorities in 2005.

During the registration process we requested information about the future use of the picture and other information that was taken, and the built-in functionalities of the seemingly innocent plastic badge. No public information or privacy policy was available upon our demands, that could indicate the purpose, processing or retention periods for the data collected. The registration personnel were obviously not properly informed and trained.

Our main concern is not only that the Summit participants lack information about the functionalities of this physical access system implemented, or that no one was able to answer questions of how the personal data would be treated after the Summit. The big problem is that system also fails to guarantee the promised high levels of security while introducing the possibility of constant surveillance of the representatives of civil society, many of whom are critical of certain governments and regimes. Sharing this data with any third party would be putting civil society participants at risk, but this threat is made concrete in the context of WSIS by considering the potential impact of sharing the data collected with the Tunisian government in charge of organizing the event in 2005.

That a system like this gets implemented without a transparent and open discussion amounts to a real threat for the participants themselves, and for our Information Society as a whole.

More information is available at:

-----  
<http://www.contra.info/wsisis>  
email: [wsisis@contra.info](mailto:wsisis@contra.info)

=====  
Contact persons:

=====  
>>Ass. Prof. Dr. Alberto Escudero-Pascual, Researcher in Computer Security and Privacy, Royal Institute of Technology, Stockholm, Sweden (EN, SP) Tel: + 41786677843 , +46 702867989

>>George Danezis, Researcher in Privacy Enhancing Technologies and Computer Security, Cambridge University, UK. (FR, EN, GR)

>>Stephane Koch, President Internet Society Geneva, Executive Master of Economic Crime Investigations, Geneva, Switzerland. (FR, EN) Tel: +41 79 607 57 33

-----  
NOTES TO EDITORS

-----  
>>The World Summit of Information Society has contracted SportAccess, a Company of Kudelski Group, as the main responsible of an integrated solution for physical access control solution during the United Nations Summit of

Information Society. The MultiSAK system has already been deployed in other meetings as the World Economic Forum in previous years and was globally designed and developed by NagraCard and NagraID.

>>The procedures of how personal data is being handled during WSIS break the principles of the Swiss Federal Law on Data Protection of June 1992 [2], the European Union Data Protection Directive 95/46/EC [3] and the United Nation guidelines concerning Computerized personal data files adopted by the General Assembly on December 1990.

>>The Electronic Privacy Information Center [1] has an extensive news archive and background material on the subject of privacy threats and RfTags. Usage of RfTags in supermarkets, to tag products for purposes of stock management and security, has already attracted oppositions on privacy grounds by CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) [5] and has lead to campaigns for customer boycott of tagged products [6].

## REFERENCES

[1] Electronic Privacy Information Center Website about RFID Identification  
<http://www.epic.org/privacy/rfid/>

[2] Swiss Federal Law on Data Protection,  
<http://www.edsb.ch/e/gesetz/schweiz/index.htm>

[3] European Union Data Protection Directive,  
[http://europa.eu.int/comm/internal\\_market/privacy/index\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/index_en.htm)

[4] Guidelines for the Regulation of Computerized Personal Data Files,  
<http://www.unhchr.ch/html/menu3/b/71.htm>

[5] - <http://www.nocards.org/AutoID/overview.shtml>

[6]The Boycott Gillette Campaign - <http://www.boycottgillette.org/>

Posted by markus at December 10, 2003 03:45 PM

## Comments

I always feel like somebody's watching me.

Posted by: [dave](#) at December 21, 2003 06:30 AM

thanks

Posted by: [penis enlargement pills](#) at January 12, 2004 12:35 AM

Hello

Posted by: [eMule](#) at January 13, 2004 04:41 PM

cool

Posted by: [Paris](#) at January 19, 2004 10:07 AM

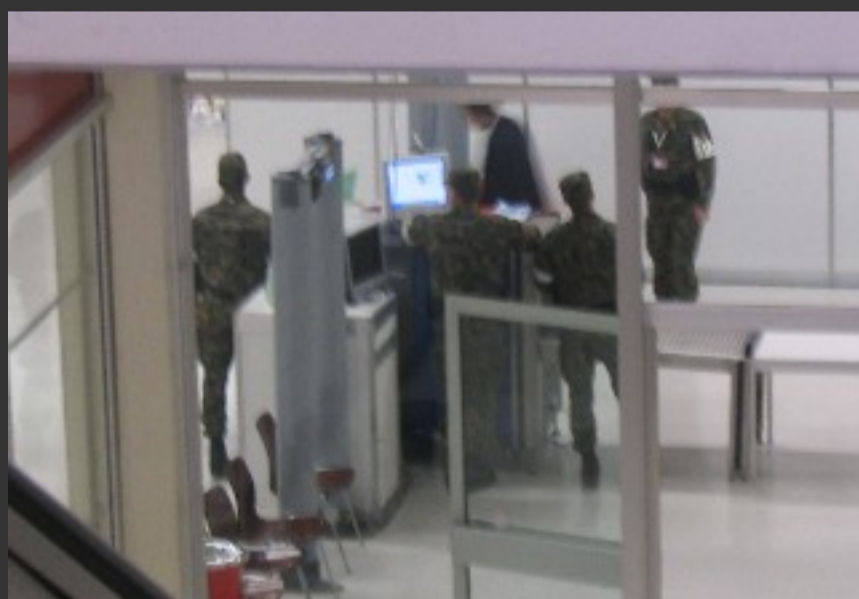
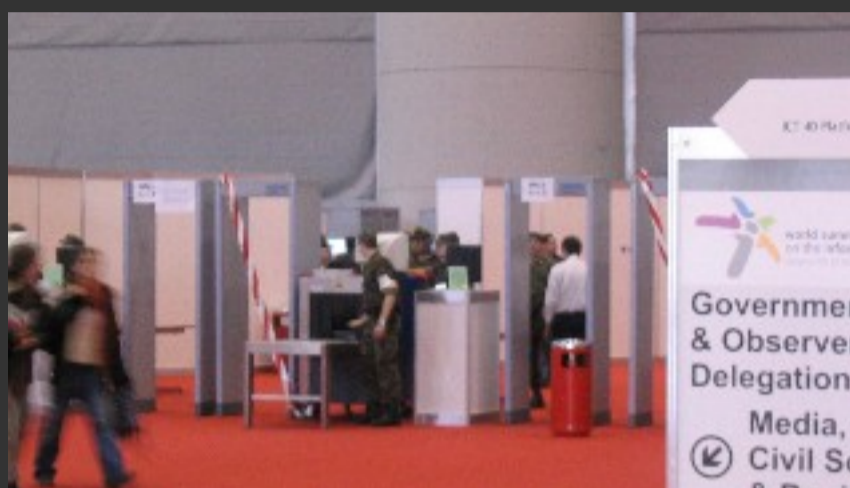
# German Civil Society at WSIS

« [Online Guide to Human Rights from Korean NGO](#) | [Main](#) | [Bericht vom Mittwoch, Teil 2](#) »

December 10, 2003

## A Glimpse Into The Security Features

A quick glance at the security control both at the entrance as well the access to the upper floor.



The security at the Summit is quite impressive at first sight so I thought it might be interesting to readers. Registration is mandatory for all participants and results in a personal RFID badge with one's name, entity and picture printed upon and the storage of named data into a central database.

Entrance to the Palexpo congress is limited to persons with a badge. There is a main gate that separates the Summit security zone from the perimeter. Members of the [Swiss armed forces](#) in full uniform check the baggage with Röntgen scanners from [Smith Heimann Systems](#), a subsidiary to [Rheinmetall AG](#). Their system is also commonly used at most European airports. To enter the Summit, the badge is pressed against a RFID reader which results in one's data to be displayed on an LCD screen, which in turn is visually compared by the security personnel against the badge and the delegate's face, while stepping through a metal detector.

This procedure also has to be repeated upon ascending to the plenary room level.

Posted by andreas at December 10, 2003 07:26 PM

## Comments

Stop by the UN Volunteers telecenter and say hi!! Certain people in the booth who shall remain nameless are deeply impressed with this web site -- online activism at its best!!!





## Han hackejat la WSIS

Revoltes / Hackers

**Data:** 11 Des, 2003 - 12:18 AM

Què és la [WSIS](#)? Doncs segons forces [resolucions](#) d'una gent que és molt important, és una cimera transcendental. Però per a la resta de mortals no és més que una d'aquestes trobades on gent encorbatada parlen i parlen... oficialment es diu 'Cimera Mundial sobre la Societat de la Informació' (en anglès). Segurament tenien la intenció d'ordenar el bullici d'activitat que generen les tecnologies de la informació i la comunicació, però han fet el ridícul: un grup de hackers els ha passat la mà per la cara.

Les noves tecnologies no poden ser controlades per polítics i realment no ho són, ho hem tornat a veure avui, però els hackers [sempre ho han dit](#): La informació vol ser lliure!

El grup en qüestió ha aconseguit saltar-se les mesures de seguretat per passejar-se entre els mandataris del món. El sistema consistia en una tarja de plàstic que conté un xip (una SmartCard) amb la informació personal i amb capacitat per ser localitzat en qualsevol punt del recinte gràcies a uns detectors que poden estar amagats (o no) en qualsevol lloc. D'aquesta manera, l'organització pot saber en qualsevol moment què està fent cada persona, les xerrades a les que ha anat, les persones amb les que està...

Això és il·legal, qualsevol mètode de control que es vulgui utilitzar ha de ser autoritzat per la persona vigilada, en aquest cas, els acreditats no eren informats de que les seves dades eren en una base de dades.

Així doncs, han matat dos ocells d'un sol tret, d'una banda, han demostrat que el sistema de les targetes és patètic i per l'altra, que és il·legal perquè pot emmagatzemar dades personals sense el consentiment de "l'afectat".

Tal i com expliquen a la [nota de premsa](#) no han utilitzat més tecnologia que la que tu utilitzes per llegir aquest text: un navegador, ha estat un exemple magnífic d'enginyeria social. Només amb la informació de la pàgina de la cimera n'han tingut prou per colar-se.

Podeu llegir la nota publicada per [Suburbia](#), la [nota de premsa](#) dels hacktivistes on ho expliquen amb pels i detalls o veure'n [imatges](#). Hi ha una [Contracimera](#) a Madrid, organitza el [Hacklab WH2001](#), alias Cielito Lindo, si hi vols anar, espavila't que s'acaba el dissabte.

---

Aquest article prové de \_el5ud.Org  
<http://www.elsud.org/>

Adreça web de la notícia:  
<http://www.elsud.org/modules.php?op=modload&name=News&file=article&sid=914>

[La gente](#)[La sociedad](#)[El ambiente](#)[La comunicación](#)[La globalización](#)

## Noticia Amenaza a la privacidad de los participantes

Nuevas Tecnologías de la Información - Miércoles 10/12/2003

La Cumbre mundial de la sociedad de la información ha contratado a SportAccess, una compañía del grupo Kudelski, como el responsable principal de una solución integrada para el control de acceso físico a la Cumbre organizada por Naciones Unidas. El sistema, que ha sido utilizado con anterioridad en otras cumbres como el Forum Económico Mundial, ha sido desarrollado por NagraCard y NagraID.

Un trabajo inicial realizado por un grupo independiente de expertos atendiendo la CMSI ha encontrado importantes fallos de diseño en el sistema propuesto desde el punto de vista técnico y legal.

El carné de identificación que se obtiene durante el proceso de registro en la Cumbre esconde un chip inteligente (SmartCard). El carné se obtiene después de mostrar un documento de identidad y dejar que una web cam tome una foto de cada participante. Lo que parece en principio una simple tarjeta de plástico es en realidad un SmartCard y un Rftag que se comunica con un lector de radiofrecuencia que puede estar ubicado en la entrada de una sala de conferencias o un ascensor. La tecnología, que también incluye una tinta segura especial en la tarjeta, permite la identificación remota de los participantes o grupo de participantes atendiendo cierto evento en un lugar concreto de la Cumbre.

Los datos personales del participante, incluida su fotografía, no se almacenan en la tarjeta sino en una base de datos centralizada. La solución permite por lo tanto monitorear cada uno de los movimientos de los participantes, incluyendo la posibilidad de saber si atienden determinada sesión, o establecer las relaciones de los participantes y sus interacciones.

Debido a que todos los datos personales, que no solo incluye la fotografía sino cada una de las transacciones asociadas a cierto individuo, se almacenan en una base de datos centralizada, partes de la base de datos o su totalidad pueden ser replicados y transferidos a futuros eventos como la siguiente Cumbre que será hospedada por el gobierno de Túnez en 2005.

Con la única intención de mostrar lo delicado del asunto, durante el transcurso de la investigación integrantes del grupo fueron capaces de registrarse en la Cumbre y obtener una tarjeta de acreditación

### Información adicional de Choike

#### ➤ Informes especiales

#### - **Cumbre de la Sociedad de la Información (CMSI)**

Una oportunidad para construir una sociedad de la información más equitativa

después de mostrar tan sólo un documento de identificación falso. No se les pidió otra información como la confirmación del número de registro a la conferencia. Los datos necesarios para confeccionar el documento fueron obtenidos de la web de la Cumbre. Durante el proceso de registro se preguntó acerca del uso de la información personal y las funcionalidades incluidas en el carné de plástico de los asistentes, pero no se logró obtener ninguna información sobre el sistema o la política de privacidad del evento.

La preocupación principal no es sólo la falta de información que los participantes reciben acerca del sistema de control de acceso al evento o que nadie fuera capaz de contestar cómo los datos personales iban a ser tratados en el futuro; el problema principal es que el sistema en realidad no introduce una verdadera seguridad y por el contrario introduce la posibilidad de monitorear a los representantes de la sociedad civil.

Los firmantes de la denuncia -Prof. Dr. Alberto Escudero-Pascual del Royal Institute of Technology de Estocolmo, Suecia; Stephane Koch, Presidente de la Internet Society Geneva; y George Danezis, de la Universidad de Cambridge, Inglaterra- consideraron una amenaza para los participantes y para el total de la sociedad de la información que sistemas como éste se implementen sin una discusión transparente y abierta.

Más información (en inglés)

<http://www.contra.info/wsis>  
[wsis@contra.info](mailto:wsis@contra.info)

=====

Contactos:

=====

>>Ass. Prof. Dr. Alberto Escudero-Pascual, Researcher in Computer Security and Privacy, Royal Institute of Technology, Stockholm, Sweden (EN, SP) Tel: + 41786677843 , +46 702867989

>>George Danezis, Researcher in Privacy Enhancing Technologies and Computer Security, Cambridge University, UK. (FR, EN, GR)

>>Stephane Koch, President Internet Society Geneva, Executive Master of Economic Crime Investigations, Geneva, Switzerland. (FR, EN) Tel: +41 79 607 57 33

## REFERENCIAS

[1] [Electronic Privacy Information Center Website about RFID Identification](#)

[2] [Swiss Federal Law on Data Protection](#)

[3] [European Union Data Protection Directive](#)

[4] [Guidelines for the Regulation of Computerized Personal Data Files](#)

[5] [CASPIAN - Consumers Against Supermarket Privacy Invasion and Numbering](#)

[6] [The Boycott Gillette Campaign](#)



www planet  
POWERED BY:  
Google zoek

## katernen

Binnenland

Buitenland

Economie

## ▼ Planet multimedia

content

nettech

mobiel

it en telecom

e-commerce

## ▶ Sport

Wetenschap

## extra's

▶ Dossiers

Cartoons

▶ Columns

24 uur

▶ Radionieuws

## Inbraak in toegangssysteem WSIS-conferentie

Gepubliceerd op donderdag 11 december 2003

**(P7) Hackers hebben de beveiliging voor toegang tot de World Summit on the Information Society weten te forceren, de belangrijkste mondiale politieke ICT-bijeenkomst dit jaar. Daardoor kwam ook een grote privacy-inbreuk aan het licht.**

De [WSIS](#) begon gisteren. Een groep Spaanse technische deskundigen van [Nodo50](#) beschrijft op [Indymedia](#) in geuren en kleuren hun inbraak, elders [vertaald in het Engels](#).

De hack is aangegrepen door drie belangrijke wetenschappers om een [klacht te ventileren](#) over de beveiliging en privacy tijdens de WSIS. Het ging om de Spanjaard Alberto Escudero-Pascual, wetenschapper van het Koninklijk Instituut voor Technologie in Stockholm, Stephane Koch, voorzitter van de Internet Society in Geneve, en George Danezis, onderzoeker in Cambridge.

Met een namaak plastic kaart met namen die van de website van de WSIS waren geplukt kregen ze toegang tot de bijeenkomst. De beelden van de webcams waren voor derden te zien.

De inbraak bracht ook aan het licht dat de ITU met gebruik van RFID-chips voor elke deelnemer en het vastleggen van bewegingen daarvan in een centraal databanksysteem een totaal beeld krijgt van de bewegingen van alle bezoekers. Nergens vonden de professoren hierover iets in een privacybeleid van de organisatie.

Het beveiligingslek is een klap voor de internationale telecom-unie (ITU) die zo haar best doet om het beheer van internet naar zich toe te trekken, mede uit overwegingen van beveiliging.

(P7)

[reageer](#)[stuur door](#)[print](#)

### headlines

- ▶ 22:13 Microsoft laat Nederlandse site ...
- ▶ 18:43 Fusiepoging RTV Noord-Holland en...
- ▶ 18:41 Martha Stewart vertrekt bij eige...
- ▶ 18:40 Computervirus vaker uit op vertr...
- ▶ 17:42 EU: Microsoft overtreedt mededin...
- ▶ 16:54 Slag om Amerikaanse kiezers op s...
- ▶ 15:35 Omvang internetreclame nadert 40...
- ▶ 15:02 Fotoverbod Leeuwarder Courant op...
- ▶ 14:48 Meer Elseviergeld in Zibb.nl
- ▶ 14:43 Brussel: diep wantrouwen e-commerce
- ▶ 14:20 25 procent groei online adverte...
- ▶ 14:06 Radiozenders drie minuten stil
- ▶ 12:54 Iraans tijdschrift wegens satire...
- ▶ 12:19 Base schrapte 200 banen
- ▶ 11:47 Vanaf september 2004 UMTS/vaste ...

**digitale camera?** [meer](#) →  
Je vindt 'm bij Kieskeurig

**planetclubs** [meer](#) →  
Ontmoet mensen met dezelfde interesse

Beurs AMX 378.4	Weer 13°	Verkeer 0 Files 0 Km
-----------------------	-------------	----------------------------

### boeken

[bol.com](#)

- ▶ tip Mac OS X Panther
- ▶ tip Snelgids Netwerken thuis
- ▶ tip Adobe Premiere Pro / NL + CD-ROM

### geld & carrière

Omdat een loopbaan meer is dan werk alleen.

[verder](#) →

### planet game club

eindeloos pc-games spelen via uw Planet ADSL-verbinding.

[meld u aan](#) →

### planet adsl

Kijk of ADSL bij u in de buurt mogelijk is!

postcode

huisnummer

### planet domeincheck

Check en registreer uw (bedrijfs)naam voor internet bedrijfsnaam



Konzeptuelles & Beteiligung  
Mailingliste  
Medienaktivismus  
Gedanken zu Provos & Fakes

Feature-Archiv  
Newswire-Archiv  
publizieren [/ohne verschlüsselung]



Themenseiten  
Repression  
Wohnungsnot/Squat  
Krieg+ Militarismus  
Sans-Papiers  
Medien  
G8-Évian  
WEF



Links  
Radio Rabe  
Radio LoRa  
Radar Kalender  
Egocity Squat

IMCs  
International  
www.indymedia.org

Afrika  
ambazonia  
nigeria  
südafrika

Europa  
athen  
barcelona  
baskenland  
belgien  
belgrad  
bristol  
deutschland  
estrecho/madiaq  
finnland  
frankreich  
galiza  
grossbritannien

## La sécurité de l'accès physique au SMSI

*maria, 10.12.2003 21:56*

### Une menace de données privées pour les participants

Traduit de [www.nodo50.org/wsis/](http://www.nodo50.org/wsis/)

GENÈVE, le 10 décembre 2003

Un groupe international de chercheurs indépendants qui assistent au Sommet Mondial sur la Société de l'Information (SMSI) a révélé des failles techniques et légales importantes, concernant la protection des données personnelles, dans le système de sécurité employé pour contrôler l'accès au sommet de l'ONU.

Le système non seulement ne garantit pas les niveaux élevés de sécurité promis mais offre également une possibilité de surveillance constante des représentants de la société civile. Pendant notre recherche, expliquet ils nous avons pu nous inscrire au sommet et obtenir une entrée officielle juste en montrant une fausse carte d'identité plastique et étant photographié (par une webcam), sans que d'autre document ou numéro de matricule soit requis pour obtenir le pass. Il a fallu tres peu de données personnelles pour produire une fause identité et donc pour s'enregistrer - càd . un nom de participant inscrit via le site du SMSI.

Mais c'e n'est que la moitié de l'histoire.



Les badges officiels du Sommet, qui sont en plastique et ont la taille d'une carte de crédit, cachent une "RFID smart card" [ 1 ] - une puce cachée qui peut communiquer son information par fréquence radio. Il est équipé d'un identifiant unique liée au participant qui le porte, et une étiquette de fréquence radio (RFID) qui peut "être lue" en passat a proximité d'un lecteur.

Ces sondes peuvent être situées n'importe où, sur des distributeurs automatiques comme aux entrées d'un lieu spécifique de réunion, permettant l'identification et le cheminement à distance des participants, ou des groupes de participants, assistant à l'événement. Les données concernant la personne qui porte cette carte (détails, autorisation d'accès, information de compte, photographie personnelle etc...) ne sont pas stockées sur la puce elle-même, mais sont gérés par une base de données relationnelle centralisée. Cette solution permet au système centralisé de surveiller étroitement chaque déplacement des participants à l'entrée du centre de conférence, l'interaction humaine des participants et leur rapport, ou d'employer des techniques d'extraction de données. Le système peut potentiellement être étendu aux déplacements des participants dans le sommet et détecter leur présence à une session particulière. Puisque toutes les données personnelles sont stockées dans une base de données centralisée, n'importe quelle partie de la base de données peut être dupliquée localement, ou être transférée pour de futurs événements - par exemple le prochain sommet de WSIS accueilli par les autorités tunisiennes en 2005.

Pendant le procédé d'enregistrement nous avons demandé d'un ton innocent des informations sur la future utilisation de la photo et toute autre information qui a été prise, et les fonctionnalités intégrées dans le badge en plastique. Aucune information ou politique publique sur les données privées ne nous a été communiquée en réponse de nos questions, ce qui aurait pu clarifier le but, le traitement ou la rétention des données rassemblées. Le personnel d'enregistrement évidemment n'a pas été correctement informé et n'a pas été formé. Notre souci principal est non seulement que les participants au Sommet ne sont pas au courant de ces informations sur les fonctionnalités de ce système physique d'accès mis en place, mais que personne n'était capable de répondre aux questions sur la façon dont ces données personnelles vont être traitées après le sommet.

Le grand problème est que le système ne garantit pas les niveaux élevés de la sécurité promis tout en présentant une possibilité de surveillance constante des représentants de la société civile, dot beaucoup critiquent les pour gouvernements et régimes. Le partage de ces données avec n'importe quel tiers mettrait les participants de la société civile en danger, mais cette menace devient concrete dans le contexte du WSIS si on considère l'impact potentiel du partage des données rassemblées avec le gouvernement tunisien responsable d'organiser l'événement en 2005.

Qu'un système comme celui ci soit mis en application sans transparence et ouverture de discussion à une vraie menace pour les participants eux-mêmes, et pour notre société de l'information dans l'ensemble.

Plus d'informations et photos

- irland
- istanbul
- italien
- lancaster
- liege
- lille
- madrid
- niederlande
- nizza
- norwegen
- österreich
- paris
- polen
- portugal
- russland
- schottland
- schweden
- schweiz
- thessaloniki
- tschechien/prag
- ungarn
- wales
- west flandern
- zypern

- Kanada**
- alberta
- hamilton
- maritimes
- montreal
- ontario
- ottawa
- quebec
- thunderbay
- vancouver
- victoria
- windsor

- Lateinamerika**
- argentinien
- bolivien
- brasilien
- chiapas
- chile
- ecuador
- kolumbien
- mexiko
- peru
- puerto rico
- qollasuyu
- rosario
- sonora
- tijuana
- uruguay

- West-Asien**
- beirut
- israel
- jerusalem

- Ost-Asien**
- japan

- Süd-Asien**
- indien
- mumbai

- Pazifik/Oceania**
- adelaide
- aotearoa

## Ergänze diesen Artikel (ohne Verschlüsselung)

**WSIS ne fiche pas, WSIS contrôle les fiches**

11.12.2003 09:46

Données personnelles requises : nom, prénom, à quel titre et pour quelle entité on est présent. Numéro de passeport ou de carte d'identité.

C'est tout.

Il est évident que cette base de données est contrôlée à l'aide de celles, plus officielles, des états civils de chaque pays concerné. Ils demandent si peu de renseignements.

Ce n'est pas cette base de données là qui me semble inquiétante. Ce qui est inquiétant c'est cette \*globalisation\* des fichiers d'état civil à l'occasion de ce forum.

Il faut dire aussi que les demandes d'accréditation devaient être déposées depuis des mois et que l'ONG (ou autre exposant ...) devait être accrédité pour pouvoir faire accréditer les représentants qu'elle désire envoyer.

La fouille très poussée est la même que dans les aéroports.

Et pour le reste, y'a autant de militaires et de policiers que de participants & visiteurs à ce SMSI.

Quelques images ici, pas encore de commentaires.

La conférence Ramonet-freire-Tahar ayant été très chaude, surtout après le départ de Ignacio Ramonet, je remet mon récit de tout cela à plus tard.

Bien qu'ayant eu quelques petits problèmes pour obtenir mon accréditation, sous des prétextes un peu foireux de leur part, après qu'ils aient rapté ma carte d'identité pendant un quart d'heure ainsi que mon accréditation, ils m'ont donné mon badge-à-puce.

J'y suis en tant que membre d'une ONG.

Premières impressions : le problème de la Tunisie, choisie pour 2005, est manifestement un problème.

Houleux échanges entre groupes divergeants (dont certains proches du gouvernement Tunisien, selon toutes probabilité.

Aujourd'hui, c'est le forum des droits sur internet, et y'a Richard Stallman.

nom

☞ Homepage:: [http://www.anti-g8.org/breve.php3?id\\_breve=161](http://www.anti-g8.org/breve.php3?id_breve=161)

# Furd Log

Intellectual Property: Technology, Culture, Policy

**Tuesday, December 30**

## [Oh, Yeah – That RIAA Strategy Is Working Well](#) [9:36 pm]

From the BBC: [Music sharing tops net searches](#)

More people looked for information about the file-swapping program Kazaa than anything else on the net in 2003, according to search site Yahoo.

It beat Harry Potter, Britney Spears and Eminem to top the list of the year's most popular searched-for terms.

It shows that despite legal moves by the recording industry to clamp down on illegal music swapping, surfers are still interested in such software.

[permalink to just this entry](#)

## [A Wrinkle on the Amazon Scan System](#) [4:14 pm]

Via [beSpecific](#) – [Amazon page search alarms writers of cookbooks, references](#) [pdf]

On Oct. 23, Amazon.com initiated a new function called “Search Inside the Book.” Launched in conjunction with publishers, the program allows customers to search every word of every page of about 120,000 books - including dozens of cookbooks. It has been called “the Google of books.”

Or, for cooks, a sort of Google meets Epicurious, the Web site that provides free recipes from Bon Appetit and Gourmet, among other food publications.

Though visitors to the Amazon site are limited to reading only 20 percent of any book included in “Search Inside the Book” (a restriction that would prohibit a reader from finishing a best-selling novel, for example), they could easily pull out a recipe from a cookbook.

[...] Paul Aiken, executive director of the Authors Guild, an advocacy group for authors, has opposed the search function since its inception, describing it as a possible copyright infringement. Of particular relevance, Aiken explains, are reference-style books that contain a compact unit of marketable information on an individual page, such as cookbooks and travel books.

As those who've read Lessig's *Code* know, you can't copyright recipes, but you can copyright a book containing recipes. Similarly, you cannot copyright the data in an almanac, but you can copyright the almanac. And, depending on how you interpret the EU's copyrighting of databases, it may well be that you can copyright data there, too.

Speaking as someone who's gone to a bookstore to peruse cookbooks for ideas, was I really breaking the law? What about writing down a recipe from a library book? It seems to me that, once again, the seductive power of monopoly (awarded under copyright) is leading to nonsensical claims. Time to get back to that [article on metaphor](#), methinks....

[permalink to just this entry](#)

## [Dave Barry's 2003 Wrapup](#) [3:38 pm]

From the Washington Post ([Between Iraq and a Hard Place](#) [pdf]) includes this July highlight:

In entertainment news, CNN, concerned about flagging viewer interest in the Laci Peterson format, switches to “All Kobe, All the Time.” The music industry, in what is seen as a last-ditch effort to halt the sharing of music files on the Internet, asks a federal judge to issue an injunction against “the possession or use of electricity.”

[permalink to just this entry](#)

## [A Provocative Question](#) [1:32 pm]

How well do metaphors help us understand the Internet? [Gore, Gibson, and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary](#) [via [Legal Theory Blog](#) (note there’s something wrong with his clock, or else he’s crossed the International Date Line without telling us <G>)]

This paper seeks to explore the evolution of metaphorical inferences as applied to the Internet within legal commentary and judicial opinion. Three metaphors in particular will be examined (though this is not an exhaustive analysis by any means): the information superhighway, cyberspace, and the Internet as “real” space. Given the Internet’s ongoing evolution as an unstable and ever-changing technology, courts and commentators have faced perpetual difficulty in mapping metaphors to it. Changing social constructions of the Internet as necessitated by its evolving underlying technological architecture have supported, or conversely eroded, a particular metaphor’s literal congruence with reality. The purpose of this paper is not to normatively assess what metaphor (if any) *ought* to be applied to the Internet in legal analysis, rather it is to make transparent the different conceptions of the Internet courts and commentators are *sub silentio* employing, and the various sociological, technological, and ideological conceptions of the world that support them.

[permalink to just this entry](#)

## [Benny Evangelista’s Year in Review](#) [1:16 pm]

[Online music finally starts to rock ‘n’ roll: Industry punishes downloaders while getting into the act itself](#)

In 2003, the struggling record industry found two ways to get consumers to pay for online music – by enticing them with new, licensed Web services or scaring a chosen few to settle potentially expensive lawsuits.

[permalink to just this entry](#)

## [US Bicycles Invade Europe](#) [11:14 am]

Sorry – this is terribly off-topic, but of particular interest to me as I start to think about getting back into cycling shape: [U.S. Bike Makers Seek Dominance in Europe](#)

Faced with rapidly declining sales and shrinking margins on mountain bikes, American bicycle makers are looking to generate growth in Europe, where road cycling remains a popular spectator sports. Trade figures do not distinguish between sales of road bikes, which have thinner tires and light frames and are meant for use on pavement, and mountain bikes, which are heavier and equipped for off-road use. However, Lou Mazzante, the managing editor of Bicycle Retailer and Industry News, a trade publication, said he thinks that three American companies - Trek, Cannondale and Specialized - sell about 50,000 complete, high-end road bicycles a year in Europe at the moment, up from virtually none a decade ago.

[permalink to just this entry](#)

## Monday, December 29

### [A Little Copyright Wrapup at GrokLaw](#) [10:25 pm]

Following up to an earlier post ([A Setback for the Second Enclosure Movement](#)), we get this nice summary over at GrokLaw: [What Can’t You Copyright?](#) – plus pointers to Lessig comments as well.

[permalink to just this entry](#)



## [Mattel v. Walking Mountain](#) [8:15 pm]

An entertaining decision from the Ninth Circuit: [Mattel v. Walking Mountain Productions](#) ([Findlaw's link](#)) (summarized in this Reuters news item: [Court Rules Nude Barbie Photos Are Free Speech](#)) – see a sample of "Food Chain Barbie" at Illegal Art – [www.creativefreedomdefense.org](#) is his WWW site, but it's timing out tonight – a Googling finds [the exhibit](#) at his domain, but it's not responding.

A federal appeals court on Monday upheld a Utah artist's right to make nude photos of Barbie dolls being menaced by kitchen appliances.

Noting the image of Barbie dolls is "ripe for social comment," a three judge panel of the 9th Circuit Court of Appeals rejected toymaker Mattel Inc.'s appeal of a lower court ruling in favor of lampooning the popular doll.

The San Francisco-based appeals court ruled that naked photos of Barbie made by Kanab, Utah, artist Thomas Forsythe were meant to be a parody and could not affect demand for Mattel products.

Even better, from the opinion:

On cross-appeal, we VACATE and REMAND the Los Angeles federal district court's decision to deny Forsythe attorney's fees under the Lanham and Copyright Acts. [slip op. p. 18207]

Update: From SFGate – [Appeals court tosses lawsuit targeting Barbie lamponer](#); also, the Scrivener's Error writeup: [More Barbie News](#)

[permalink to just this entry](#)

## [Another Set of Data Points](#) [4:31 pm]

More on the stalling of internet deployment, and some indication of how well the RIAA's battle is going [via [beSpecific](#)] – from the Christian Science Monitor: [The Internet hasn't reeled in everyone yet](#)

After spiking in the 1990s and early 2000s, the percentage of adult Americans online has leveled off in the past two years at 63 percent, says a new study from the Pew Internet & American Life Project. That percentage is expected eventually to rise, but not as quickly as some had imagined.

"It's no longer the case that the Internet population is growing by leaps and bounds," says Lee Rainie, director of the Pew project. However, "the Internet is eventually going to become as important and universal a technology as telephones and televisions are now."

Ninety-four percent of American homes today have telephones; 98 percent have TVs. "The Internet is eventually going to get to that level," he predicts, "but it's going to take at least 10 years - or maybe even 15 or 20."

[...] One key barrier slowing Internet growth is the lack of broadband connections in some areas, says Phillipa Gamse, an e-business strategy consultant in Santa Cruz, Calif. Broadband allows users to move around the Internet faster, doesn't tie up the phone line, and, perhaps most important, can be left on all the time, like other appliances.

From the Pew Study: [America's Online Pursuits: The changing picture of who's online and what they do](#) – [Hobby and Entertainment Activities](#)

*About a third of users download music files.*

- 32% of Internet users have downloaded music, as of October 2002.
- That represents growth of 71% from 21 million Americans who had downloaded music as of the summer of 2000, to 36 million who had done so as of October 2002.
- The number of users who download on a typical day doubled from 3 million to 6 million between 2000 and 2002.
- Online men are more likely than women to download music.
- This activity is particularly appealing to online minorities.
- Young adults and teens are the likely downloaders.
- There is a higher proportion of downloaders among those with modest household incomes and with high school

diplomas.

- Those with broadband connections are more likely than others to download music.

[...] Wired young adults have undoubtedly driven the growth of music downloading more than any other adult age group. As we have reported previously, college students, represented in the 18- to 29-year-old demographic, are twice as likely to have downloaded music compared to the general population and they are three times as likely to do so on any given day. College students often have free access to high-speed Internet connections on campus and have utilized those resources to become pioneers and heavy users of file-sharing technologies. The older an Internet user, the less likely he or she is to have downloaded music. While 54% of 18- to 29-year-olds had downloaded music in October 2002, just 29% of 30- to 49-year-olds had done so.

Children and teens have been even more voracious downloaders. In a special survey of 754 children between the ages of 12 and 17 that we conducted in late 2000, we found that 53% of online children had downloaded music. For comparison's sake, only 42% of 18- to 29-year-olds said they had done this. Considering the growth that has occurred across all age groups between 2000 and 2002, it is likely that number of children downloading music has also grown.

See also [A Slowdown In Broadband Deployment](#)

[permalink to just this entry](#)

## [More on Exclusive Music Deals and Mega-Retailers](#) [2:32 pm]

[Big Stores Make Exclusive Deals to Bring in Music Buyers](#) (See also the article in [The Music Biz – Then and Now](#) from November – see the PDF, the Globe link has expired)

The exclusive deals are being offered as mass marketers are seeing their share of the music business grow. Discount stores like Wal-Mart accounted for only 13.5 percent of music sales in 1994, said Clark Benson, the chief executive of the Almighty Institute of Music Retail, a Los Angeles-based company that sells data about retailers to record labels. This year the figure is 34.8 percent. Billboard and its corporate sibling Nielsen SoundScan lump electronics chains like Best Buy and Circuit City with traditional music stores. Adding their sales to the other mass marketers would probably raise that group's total to more than 50 percent, said Geoff Mayfield, the director for charts and senior analyst at Billboard.

For the retailers, the deals are as much about using the artists' appeal to lure customers as they are about selling CD's and DVD's. For the musicians, the deals are less about sales than about promotional campaigns well beyond anything offered by record companies even in their glory days.

For example, Target promoted its exclusive seven-song Bon Jovi CD with an extensive television campaign. In the 30-second spot - which cost \$1 million to produce, the band's management said - snippets from a studio performance of a song on Bon Jovi's new full-priced CD were intercut with footage of band members chatting about the meaning of the song. Best Buy started a similarly ambitious television campaign for its Rolling Stones DVD set last month.

"If you look at the Target commercial, that's an ad for Bon Jovi and they just stuck their little circle on at the end," said Bruce Kirkland, one of the two principals at Bon Jovi Management.

[permalink to just this entry](#)

## [A New DVD Format Fight](#) [9:55 am]

[Heavyweights Are Choosing Sides in Battle Over Next DVD Format](#) [pdf] - a subtle story with a host of conflicting interests. With IP at the center, but also the issue of what might happen if either (a) the Chinese decide to play hardball with technology restrictions and (b) what the PC business might bring to the picture. This should be a really interesting fight – on many levels. (Slashdot discussion: [Tech Titans Prepare to Battle Over Next DVD Format](#))

The new discs and their players will not be widely available until at least 2005, but already the world's largest electronics, computer and entertainment companies are embroiled in a multibillion-dollar fight over whose technology will become an industry standard.

[...] Beyond the technical details like tracking speed and tilt is a serious tussle over how to divide - and protect - the billions

of dollars in royalties from the licensing of this technology and the content sold on the discs. Also at stake is an effort by electronics makers to prevent emerging Chinese rivals and well-established Silicon Valley computer makers from making significant inroads into the home entertainment business.

“This is a very intense conflict over intellectual property,” said Warren N. Lieberfarb, a driving force behind the development of the original DVD format. It has the added overlay, he said, “of the Japanese, Korean and European consumer electronics industries fearing China’s aggressively emerging consumer electronics industry as well as the PC industry.”

[...] Sony and its allies dismiss claims that their technology is too expensive, saying that the cost per disc will naturally fall as production takes off. They also say their rewriteable discs are what consumers really want because they can be used not only to play movies but also to record high-definition digital television programming, now available selectively in the United States and offered on a limited basis in Japan starting this month.

[...] Copyright infringement is another worry. After the rapid spread of illegally copied DVDs, Hollywood is pushing both technical groups to come up with new security measures to protect their movies. Neither group has developed a prototype that satisfies the movie industry - a major impediment to a commercial launch.

“We are very much focused on both picture quality and content protection,” said Peter Murphy, senior executive vice president and chief strategic officer at the Walt Disney Company, which has about one-fourth of the home video market. “The consumer electronics manufacturers can come up with the technical standards for the next-generation discs, but unless we also agree on the content protection standards, many of the studios may choose to wait before releasing content in the new format.”

Also lurking nearby are giants like Microsoft, I.B.M. and Intel, which are eager to work their way into family rooms by promoting their technology for use in set-top boxes, DVD players and digital video recorders with hard disk drives. American computer makers, adept at producing hardware on thin margins by building sophisticated global supply chains, could also develop competing products, turning television into just another function of the home computer.

[permalink to just this entry](#)

## [A Look at What’s Coming in 2004](#) [9:45 am]

[Media and Technology in 2004](#) (Slashdot discussion: [NYT: 14 Media & Technology Convergence Trends](#))

The convergence of media and technology, long predicted but not yet fulfilled, is at last showing signs of happening - with high-speed Internet access making much of it possible. With more American households going to broadband, faster Internet connections are changing the movie, music, telephone, computer and cable businesses.

The following entry is one of the topics raised in this article. Others include:

- [With CD Sales Slipping, the DVD Steps In](#) – and let’s think about what that means in terms of copy protection, DeCSS and other access controls – plus the laws to enforce these technological locks.

The industry is hardly settled on how best to entice customers with DVD’s. In addition to stand-alone packages, 50 Cent and the rocker Tom Petty have released DVD sets with bonus audio discs. Many more artists, from Metallica to Alicia Keys, have offered bonus DVD’s with their traditional CD albums.

Even the packaging is still in flux. The hip-hop duo OutKast, for instance, issued their recent DVD collection, “The Videos,” in both the jewel boxes used for CD’s and the clamshell case used for movie DVD’s.

Label executives hope to find clues in these numbers on how to drive DVD sales in the new year.

“Because of the plethora of releases this year, there’s certainly a lot of data which we’re in the middle of combing over now to make some decisions about what we’re going to be doing,” Mr. Katz said.

- [Personal Video Recorders: Executives Plan Now to Deal With Popularity](#)

Personal video recorders, which can easily skip over television commercials, may not yet be in most American homes, but they are certainly on the minds of advertising executives.

[...] “The challenges presented by TiVo are obvious,” Mr. [David ] Ernst [of Media Initiative North America] said. “Yet there are also opportunities to develop new types of advertising not constrained by time.”

Those include product placements within a show and interactive versions of television programs that encourage viewers to visit a Web site for more information. Initiative Media is developing advertiser-produced informational programs that could be viewed free using cable’s video-on-demand technology.

[...] Commercial-skipping is a problem for the nation’s broadcasters as well as for advertisers. A network suffers if viewers routinely skip over its promotions for programs. And if consumers record a show for later viewing, broadcasters lose the lead-in effect that helps draw viewers from popular shows to shows that follow in the lineup.

[permalink to just this entry](#)

### [More on the MPA’s “Education” Programs](#) [9:33 am]

Or propaganda – you decide. And, if that doesn’t work, there are other strategies to threaten infringers with: [Studios Fight Piracy With Education](#)

The studios say they will continue their effort to educate people on the effects that piracy has on moviegoers by threatening the fundamental economics of a popular form of entertainment. They are taking their message to grade school classrooms where volunteers teach lesson plans about the costs of illegal file sharing. Industry-sponsored advertisements are playing at movie theaters. The ads profile behind-the-scenes working people - set designers, costume makers and the like - to show that downloading hurts more than superrich entertainers.

[...] [S]ome film executives say that without drastic measures, illegal file sharing is unlikely to stop, particularly in foreign countries, like China, where pirated copies of movies are often titles more popular than the legally available fare. Ultimately, movie executives may be forced to take a cue from their music industry counterparts who caused a stir when they started suing illegal downloaders. **Only when consumers find themselves or their children facing prison, some movie executives say, will they get the message that sharing movies is a crime.** [emphasis added]

[permalink to just this entry](#)

### [USAToday on the eMusic Biz](#) [9:24 am]

It’s all about using digital music downloads to sell something else – [Via [Scripting News](#)] [2004 may see ‘bit of a gold rush’ for digital tunes](#)

Seattle-based Loudeye (LOUD) recently teamed with Microsoft (MSFT) to take advantage of the trend. The crosstown partners are offering companies a way to instantly erect their own music-download services by accessing Loudeye’s music archive using Microsoft software.

Loudeye CEO Jeff Cavins says the partnership could spur the rise of upward of 100 new digital music offerings worldwide in 2004. “It’s highly conceivable you’re about to see a bit of a gold rush around digital music,” Cavins says.

[...] Now Loudeye, which has 80 employees and annual sales of about \$13 million, has begun packaging its music archive with Microsoft’s Windows Media software and is helping companies dream up ways to use downloads to promote other products and services. “This really is a tool to drive cross-merchandising,” Cavins says.

[permalink to just this entry](#)

### [NPR’s Morning Edition](#) [9:12 am]

Today’s [Morning Edition](#) had a piece on CD copy protection, with [Prof Ed Felten](#) and Alex Halderman as well as the head of SunnComm, Peter Jacobs.

## [Music Copy Protection](#) (Javascript audio link on the NPR page)

Record labels have spent years trying to install technology on compact discs to prevent them from being illegally copied. But the vast majority of CDs are still easily burned. NPR's Rick Karr reports on the technology that keeps hackers and the recording industry at odds.

Jacobs floats the interesting theory that copy protection as absolute protection will never work, but tying adherence to copy protection to other benefits (ticket discounts, lyrics, etc.) will. Ed Felten points out that it only takes one hacker to get music files onto the P2P networks.

And, most surprisingly, there's a theory raised by [Prof. Doug Lichtman](#) (U of Chicago) that there are those who hack on the basis of purely political/moral arguments, suggesting that copying should be completely legal.

[permalink to just this entry](#)

## Sunday, December 28

### [CNet News' Roundup](#) [6:12 pm]

[2003 in Review: Playing Politics](#) - these article, plus a host of ancillary reports.

- [Court scrutinizes P2P subpoena process](#)
- [In DMCA war, a fight over privacy](#)
- [Are PCs next in Hollywood piracy battle?](#)

[permalink to just this entry](#)

### [Why Am I Not Surprised](#) [6:05 pm]

Apparently, the US Congress continues its tradition of exempting itself from legislative restrictions: [We Hate Spam, Congress Says \(Except Ours\)](#)

Even as Congress was unanimously approving a law aimed at reducing the flow of junk e-mail, members were sending out hundreds of thousands of unsolicited messages to constituents.

The spasm of activity is aimed at attracting voluntary subscribers to the lawmakers' e-mail lists, which would not be subject to House rules that normally impose a 90-day blackout before an election for taxpayer-supported Congressional mass communications.

Slashdot discussion: [Congress Loves Spam – If It's From Congress](#)

[permalink to just this entry](#)

### [From the NYTimes Least Liked Music of the Year Column](#) [6:00 pm]

#### [Tasteful Imitations and Sagging Follow-Ups](#)

*Jon Pareles, Neil Strauss, Ben Ratliff and Kelefa Sanneh listened to a lot of bad pop music in 2003; herewith, their least fond recollections.*

[...] **STRAUSS** My biggest letdown was watching the recording industry deal with downloaders. I just think it's terrible p. r. I don't see any fewer people on Kazaa. The only thing it's encouraged people to do is to take their downloaded files and not share them. But they're all still there trying to get music.

**PARELES** The recording industry keeps trying to build a wall in the ocean. They keep trying to shut down the Internet. And they think they can do it by suing 12-year-olds, when what they need is a great subscription service.

[permalink to just this entry](#)

## Saturday, December 27

### [A Look at eMusic From Wharton](#) [1:37 pm]

Via News.Com: [Online music's winners and losers](#). An odd little piece, frankly, that seems to ignore the current economics of emusic retail, which is a loss leader for everyone. Wharton's proposition that streaming is the answer seems to miss the technological alienation angle – are you really ready to rely on a company to be 24/7 available, not to mention not to mixup your playlist? And what if your hardwired DRM device fails?

Provocative, at least.....

To some extent, all the models could fly. Larry Kenswil, president of eLabs, the media and technology division of Universal Music Group, suggests that music, like movies, should be able to thrive in a wide variety of channels: "People can watch a movie (at a theater), or on video, or on a pay-per-view channel. They have a dozen ways."

Some experts, though, are betting that the ranks of the online music vendors will thin out because technology, consumer preferences and costs will conspire to create a dominant business model. Wharton marketing professor Peter S. Fader says all the signs point to the eventual emergence of streaming as that model.

For the moment, though, the models based on selling tracks and albums will predominate because that is how most people have learned to obtain music online, Fader notes. Perhaps more important, downloaded music is portable. It can be burned to a CD for listening in the car. It can be put on an MP3 player for listening while jogging or flying. But, in the end, downloading is burdensome, Fader suggests. "Obtaining the songs is a nuisance. It's a pain to download them, to organize them, to back them up."

And when you come down to it, Fader adds, people really don't care much about having physical ownership of their music. What they really care about is having access to the music they like, when and where they want it.

At least they don't purely push this Wharton-based theory. We get an opposing view from Steve Jobs himself:

Not everyone, however, agrees. Apple's Steve Jobs recently told Rolling Stone magazine that music ownership is an ingrained habit, one that will always prevail: "People don't want to buy their music as a subscription. They bought 45s, then they bought LPs, they bought cassettes, they bought 8-tracks, then they bought CDs. They're going to want to buy downloads." Jobs, of course, is the mind behind iTunes and so could be somewhat partisan. But he may have a point because even with music it is important to remember that people—especially Americans—like to own things.

Then there's the community notion (see the following FurdLog entry):

The better approach, one that will most likely have to be part of a successful business model, is to create a sense of community among buyers or subscribers—not unlike the sense of community the original Napster as well as Kazaa and Morpheus have created among their users, [Gartner's Mike] McGuire says.

[permalink to just this entry](#)

### [The New York Times' Underrated and Overrated Ideas](#) [1:26 pm]

An interesting line up: [Judging 2003's Ideas: The Most Overrated and Underrated](#)

From Underrated:

#### **Curatorial Culture**

In all the hype over Apple Computer's online music store, one fascinating new feature included in the latest version was strangely overlooked: the celebrity playlist. The digital age version of the venerable mix tape, playlists have been a central selling point of the MP3 music revolution, since creating a brand-new mix of your favorite tunes is now as easy as dragging files into a folder on your desktop. Apple's new Celebrity Playlist area in its store features collections of music assembled — with liner notes — by famous musicians: Sting, Ben Folds, Wynton Marsalis and many others.

What's potentially revolutionary here is the ability to buy a compilation of music handpicked by another individual, as opposed to the official compilations released by record labels. No doubt Apple will soon offer a feature that enables ordinary music fans to create public playlists engineered around every imaginable theme (the post-breakup collection, the happy Nick Drake songs, the underappreciated recordings of Miles Davis) and then sell those compilations via the online store. Historically, the world of commercial music has been divided between musicians and listeners, but there's long been a mostly unrewarded group in the middle: people with great taste in music — the ones who made that brilliant mix for you in college that you're still listening to. They're curators not creators, brilliant at assembling new combinations of songs rather than generating them from scratch.

*Steven Johnson, author of the forthcoming "Mind Wide Open: Your Brain and the Neuroscience of Everyday Life."*

[permalink to just this entry](#)

## [A Look at the WSIS Fallout](#) [1:12 pm]

From IPJustice [via [Legal Theory Blog](#)]: [World Summit to Create "Pay-Per-Use" Society](#)

[permalink to just this entry](#)

## [Slashdot on the MPAA's "Refined" Strategies](#) [1:02 pm]

As a followup to [The MPAA Plays "Softlee Softlee Catchee Monkey"](#), we get this Slashdot discussion: [MPAA Fights Pirates with Gentle Threats](#) – see, in particular, [Read between the lines](#)

Everybody reading the article needs to read between the lines pretty carefully on this one. While the MPAA is seemingly offering the olive branch with one hand, look at the following quotes from the article:

*Along with the warning letters, the movie industry is paying for consumer education programs and technology research, and pushing for laws and regulations that executives hope will protect their wares.*

*The most important thing for Hollywood to do now, Johnson said, is to move faster to develop the kinds of licensing agreements and protective technology*

*The path to a successful service has to involve the kind of technology that protects copyright unobtrusively,*

*Hand in hand with developing legal digital services, he recommends the kind of tough security that is built into satellite television equipment,*

This whole article reeks of DRM. They never mention it by name, but this is exactly what they have in mind, and some of the stuff highlighted above suggests DRM in hardware.

So I don't see where the MPAA has learned a damn thing, other than the blatant tactics of the RIAA don't work so they're going to try more underhanded ones. The agenda of the MPAA has NOT changed one iota.

[permalink to just this entry](#)

## Friday, December 26

### [Judge Kaplan of 2600 Fame Back On Slashdot](#) [1:35 pm]

There's an article on Slashdot today, [Court Rules Against Photographers in Copyright Suit](#), based upon an article in Photo District News

Online, [NGS Beats Infringement Rap in New York](#). Essentially, a set of photographers sued the National Geographic Society over their distribution of a CD of issues of National Geographic without compensation.

The photographers were relying upon an 11th Circuit decision, *Greenberg v. National Geographic*, but Judge Kaplan, noting that *NYTimes v. Tasini* had been decided subsequent to the 11th Circuit decision and using a different theory of infringement, elected to review in light of that decision, and concluding that a CD of page scans, even with an index, is not a new work, so the earlier agreements to publish still held.

Here is a link to the case – [Faulkner et al. v. National Geographic](#). The route taken to deciding the review the materials rather than rely upon *Greenberg* is worth a look.

The issue tendered by defendants – whether the [Complete National Geographic] CNG is a “revision” within the contemplation of Section 201( c) – requires construction of the 1976 Act in a new technological context. The question is whether a print publisher of a collective work is privileged to use the individual contributions in a digital version where (a) the individual contributions are presented in the same contexts in which they appeared in print, and (b) the digital version contains also software or other materials that did not appear in the print version. This issue is one of substantial importance to the development of copyright law and to its impact on the dissemination of knowledge. The Second Circuit, to which any appeal here would be taken, of course is a jurisdiction coordinate to that of the Eleventh Circuit. In the event of a circuit conflict, the matter likely would go to the Supreme Court. A decision on the merits here thus would promote the development of the law on this important point. [slip op. page 21]

[...] *Greenberg* resolved the revision issue by looking to the question whether the CNG contained independently copyrightable elements in addition to the previously published collective works, i.e., the *Magazine*. *Tasini* took a different approach. It focused instead on whether the individual contributions appeared in the putative revisions – the electronic databases – in the same contexts in which they appeared in the original collective works. Moreover, its reference to the microform analogy has significant implications for the CNG. Accordingly, while it perhaps is possible, as a matter of formal logic, to reconcile the holdings of *Tasini* and *Greenberg*, the difference in the Supreme Court’s approach to the revision issue nonetheless is striking. [slip op. page 23]

[...] This Court is convinced, both as a matter of law and in the exercise of discretion, that application of collateral estoppel to foreclose defendants from asserting that the CNG is a privileged revision of the *Magazine* would disserve the public interest in having the important issue presented here resolved definitively and would be inequitable. It therefore holds that defendants are not foreclosed on the revision issue by *Greenberg*.

The case upon which the photographers were depending is [Greenberg v. National Geographic](#) (some background information from some Wired News articles when the case was up for cert: [Mr. Tasini, Meet Mr. Greenberg](#) and [Magazine Appeals for CD Archive](#))

[permalink to just this entry](#)

## Thursday, December 25

### [The MPAA Plays “Softlee Softlee Catchee Monkey”](#) [11:36 am]

But will it really work in the long run? While these industries grasp for control harder and harder, it appears that some are ready to opt out altogether. This NYTimes article tries to paint a reasonable picture, but only devotes a sentence to the key point: [In Chasing Movie Pirates, Hollywood Treads Lightly](#)

While the recording industry has made headlines with a few hundred lawsuits, the movie industry has been sending out hundreds of thousands of threatening notices via e-mail messages each week to the people who make its products available on the Internet.

The music industry’s approach has contributed to a decline in downloading but has also produced a powerful public backlash, angering millions of its customers. That is one reason, among others, that Jack Valenti, head of the Motion Picture Association of America, said that his industry would not be following the music companies’ path any time soon.

“I’m not ruling out anything, but at this moment we don’t have any specific plans to sue anyone,” Mr. Valenti said. “I think we have learned from the music industry.”



The gentler threat works, said Mark Ishikawa, the chief executive of BayTSP, a company that helps the industry track down file sharers by scanning the Internet for movies and issuing the e-mail notices automatically. Fully 85 percent of those contacted “do not come back,” Mr. Ishikawa said. “We never see them again,” with no headlines and no public relations blowups.

[...] Mr. Valenti says Hollywood is doing everything it can to get ahead of the coming storm. Along with the warning letters, the movie industry is paying for consumer education programs and technology research, and pushing for laws and regulations that executives hope will protect their wares. At the industry’s urging, for example, California recently passed a law making it illegal to use a camcorder in a movie theater.

Yet experts in digital technology say Hollywood is fooling itself if it believes that its current steps will be enough, or even that they will take the industry in the right direction.

[...] **What the industry needs, technology executives say, is to look harder for tools and contracts that allow people to get the movies they want at a competitive price, rather than concentrate on actions that restrict access.** [emphasis added]

[...] The costs of adopting the wrong strategy will be high. Jeff, the movie swapper, says that despite his scare he has not changed his ways. He has gone deeper underground instead, renaming files so that movie titles would not be as easy to find with industry search software, he said. (Mr. Ishikawa of BayTSP said that the strategy would not work against his service, however.)

Jeff also says that he does not make his own trove of movies available to the world as readily. “I just watch them and delete them instead of leaving it out there,” he said. “I don’t leave the network on 24 hours a day the way I used to.”

But Mr. Davis, the former song trader, has changed his habits. He dusted off his turntable, bought a new needle and started haunting the bargain vinyl bins in junk shops, where he has discovered some treasures for a dollar a record.

“I’m really very excited about it,” he said, “because there isn’t much new to buy out there, is there?”

See this followup: [Slashdot on the MPAA’s “Refined” Strategies](#)

[permalink to just this entry](#)

## Wednesday, December 24

### [Some Economics of Digital Movie Distribution](#) [9:33 pm]

From Reuters via Yahoo!: [Coming to a Theater Near You: Digital Films](#) [gotta make a PDF]

The biggest advantage for the moviegoer, says Peter Wester, project manager for Swedish cinema chain Folkets Hus och Parker, will be most visible not on the marquee – not necessarily the screen.

A cinema can download a digital version of the film on a computer hard drive and show it as long as the audience shows up. No longer are theaters bound to the major studios’ distribution schedule, he said.

“The average rise of income for us is 25 percent after one year,” he added.

It can cost thousands of dollars for a cinema to get a Hollywood blockbuster film at or near the release date. A theater operator, therefore, often has little choice but to show the movie as often as possible before returning it to the distributor.

A digital version, because it can be easily reproduced, shipped and stored, costs less than \$20 per copy, according to cinema exhibitors. It also allows the cinema operator to free up their viewing schedule, perhaps opening up the odd week-night slot for an art-house title.

And, the build-out is expensive. It costs a cinema operator an estimated \$125,000 for the equipment and installation of a digital projector and server. The costs are decreasing, with widespread roll-out expected to halve deployment cost.

The biggest obstacle though is Hollywood. The Walt Disney Co., through its partnership with Pixar Animation Studios Inc. (Nasdaq:PIXR - news), and Warner Bros. (NYSE:TWX - news), are the only studios producing blockbusters in digital film.

[permalink to just this entry](#)

## [Slashdot's Discussion of the Internet Law Year In Review....](#) [4:17 pm]

... Has some pretty interesting comments. (see [this FurdLog post](#) for the original article URL.)

- From [One year is not enough. Look back at the last ten](#)

While everyone's caught up looking at the trees, here's what's happening in the forest: We're inching ever towards limiting the common man's access to "intellectual property" (whatever that is). In doing so we're walking away from the past five hundred years of intellectual freedom brought about by Johannes Gutenberg and Martin Luther.

This is a huge, gigantic assault on the philosophy of the Enlightenment, on which (to some extent) our country was founded and our Constitution based. Yet my impression is that most computer geeks only see the tip of the iceberg – e.g. "I can't legally play my DVDs on Linux" or "ROT13! WTF J00 AD0B3 LAM3RZ!" The strongest fight is coming from librarians. **I think librarians are the only ones to realize that, were libraries to be invented today, they would promptly be sued out of existence by the RIAA for illegal filesharing.**

- [Re:At one time](#)

It's going to be really, really disturbing, though, when we all wake up and find out that we can't run our "popup blockers", use our blacklists, and filter responses through proxies anymore. It'll be "made illegal" to alter the contents of packets that we receive from the Internet because of "intellectual property" bogosity.

It's going to be even more disturbing when we all wake up and find that none of us have "root" access on our computers anymore. All our packets on the Internet are going to be authenticated and cryptographically "secured" (i. e. "secured" from US), and the content publishers and distributors will hold all the keys.

I may be overly pessimistic now, I guess, but I feel like we can't stop it. The Internet, as we know it now, is going to be gone sooner rather than later. There will be "other internets" that will be similar to this one, but the age of a single, unified, global Internet is going to pass quickly, and idiotic legislation, content publishers and distributions, and "intellectual property" are going to be the forces that break it apart.

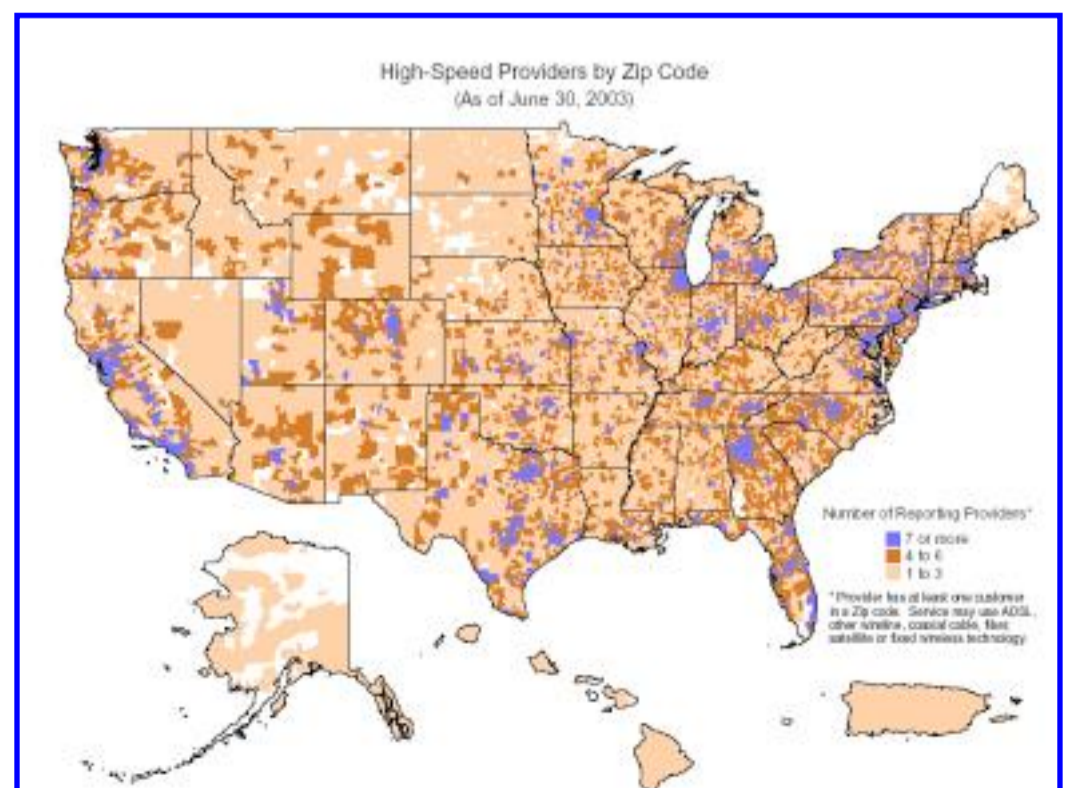
[permalink to just this entry](#)

## [A Slowdown In Broadband Deployment](#) [10:46 am]

According to the [latest statistics](#) [pdf] [reported](#) by the FCC, the rate of broadband deployment in the US declined in the most recent reporting period ([press release](#), [InfoWorld report](#)). From the InfoWorld article:

Monday's FCC report doesn't go into the policy implications of the rate of broadband growth, said an FCC spokesman. But the FCC and some members of the U.S. Congress continue to promote broadband to U.S. residents, and in April, the FCC's [Technological Advisory Council](#) attempted to examine why more U.S. residents weren't buying broadband. Among the reasons discussed then were cost and the lack of applications that needed broadband.

(I like the plot to the right, taken from the FCC report. You can see population centers, of course, but I really like seeing the formation of [BAMA](#) right before my eyes.)



## [The Question On Everyone's Mind](#) [10:22 am]

And not just because of the DVD ruling – [recall the words](#) of the DC Court of Appeals in the Verizon decision: [Will DVD acquittal mean tougher copyright laws?](#) (Note that this is a VERY extensive writeup!)

Even before the Norway case was filed, however, entertainment industry lobbyists had been pressing lawmakers in that country and elsewhere to enact tougher copyright laws, modeled on controversial U.S. legislation that makes it easier for authorities to win prison terms for people who crack encryption schemes or distribute cracking tools. If enacted, proposed legislation in Europe, Canada, Australia and Central and South America would soon hand entertainment companies similar weapons against people caught tinkering with anticopying software.

That's raising warning flags from some critics of the U.S. legislation, known as the Digital Millennium Copyright Act (DMCA), who contend the law protects content owners at the expense of consumers and software experimenters. Now, they say, that law is being exported around the globe with little debate.

"It is interesting that the court said Johansen had not broken any law, but the laws are changing," said Robin Gross, executive director of IP Justice, a nonprofit group that opposes the DMCA.

Certainly legislation will be promoted – the issue will be how to mobilize to articulate just what's wrong about the way they are framed.

[permalink to just this entry](#)

## [It's Not Just Music](#) [10:17 am]

As this article shows, the windfalls of digital distribution suggest a realignment of interests and economic power in the entertainment business – and there's no reason that the artist can't participate in that: [A 'Seinfeld' Star Will Do the DVD but Asks for Pay.](#)

"I'm not boycotting," Mr. [Michael] Richards, who played Kramer in the series, said in a telephone interview late Monday night. "I'm involved. I was never called to do an interview. I am so for the DVD coming out that I'll go on the 'Tonight' show."

But Mr. Richards said he thought he ought to be paid for taking part in the DVD project, in part because the show has been such a windfall for its creators, producers and distributors: Jerry Seinfeld, Larry David, Castle Rock Television and Columbia TriStar Home Entertainment. They will all share profits from the DVD.

Actors do not typically receive residual payments for DVD's, but this is quickly becoming a major issue in Hollywood, as DVD sales now bring in millions of dollars to those who control the rights to hit television shows and movies, far more than revenue from videocassettes.

Mr. Richards said: "I innocently asked a question. Is there some compensation? I don't believe there is. There isn't anything."

[permalink to just this entry](#)

## Tuesday, December 23

### [See, It All Worked Out In the End, Didn't It?](#) [6:18 pm]

[Statement by Assistant Attorney General R. Hewitt Pate Regarding the Closing of the Digital Music Investigation](#) - (CNet News article: [DOJ closes Net music antitrust scrutiny](#))

"The Division's substantial investigation of pressplay and MusicNet has uncovered no evidence that the major record labels' joint ventures have harmed competition or consumers of digital music. Consumers now have available to them an increasing variety of authorized outlets from which they can purchase digital music, and consumers are using those services in growing numbers.

“None of the several theories of competitive harm that the Division considered were ultimately supported by the facts. The Division found no impermissible coordination among the record labels as to the terms on which they would individually license their music to third-party services. The development of the digital music marketplace similarly belies any concerns that the record labels used their joint ventures to stifle the development of the Internet music marketplace and to protect their present positions in the promotion and distribution of prerecorded music in physical form.”

From the [Background information from the DoJ](#) we get this summary:

The Division considered in its investigation whether the major record labels used their joint ventures to suppress the growth of the Internet as a means of promoting and distributing music, in order to protect their present positions in the distribution of music on physical media, such as CDs. Proceeding collectively could have allowed the major record labels to explore the use of the Internet to promote and distribute their music, without relinquishing control over the pace and direction of those activities.

The poor quality and restrictive nature of pressplay’s and MusicNet’s services at launch in December 2001 provided some support for this theory. As time passed, however, both joint ventures released improved and more consumer-friendly versions of their services, and the major labels licensed their music to a broader array of third-party music services that compete on price and features. Consumers can now download individual songs from broad music collections offered by at least five such services, and might soon be able to choose among a dozen suppliers. The Division concluded from those developments that the major labels are not impeding the promotion and distribution of music over the Internet.

So, think about the [recent reviews](#) of the e-music services and see if you can reconcile them with the DoJ’s conclusions. And let’s not even go into the question of what the record companies were up to in the days **before** pressplay and MusicNet even existed (Napster, MP3.com and others – see John Alderman’s [Sonic Boom](#)) Or, for that matter, the [ruinous business models](#) that the emusic retailers operate under.

Then, ask yourself the following question: how do we reconcile the desire to achieve competitive markets through the application of conventional processes and investigative techniques in an era where things happen on Internet time? Particularly when our justice system lately seems to be organized around the idea that, as long as an earlier crime can be rectified with actions that yield no apparent net economic damage, then there’s nothing to prosecute (c.f., Halliburton’s gasoline price-gouging being resolved by asking for the difference between the charged price and the fair market price, rather than seeking some kind of deterring punishment?)

Bah! Humbug! Be interesting to see how much of the record of this investigation becomes public.

Update, Dec 25: the Slashdot discussion, interestingly enough, is about exactly the same issues I snarled about here – [DOJ Drops Online Music Antitrust Investigation](#)

[permalink to just this entry](#)

## [Bollywood and KaZaA](#) [2:13 pm]

Via [Slashdot](#): [Bollywood in Internet download deal](#)

India’s film makers are offering Internet movie downloads on web site Kazaa in a move that could lower costs and boost revenues in Bollywood, the world’s most prolific film production centre.

Some 35 producers will be able to sell movies using Kazaa, a file-sharing program owned by Australia’s Sharman Networks, according to company statement.

“In a distribution deal struck between Sharman’s partner Altnet... and IndiaFM.com, one of the most popular Bollywood entertainment sites, Kazaa’s estimated 60 million global users will gain access to previously unavailable content,” the statement said.

[permalink to just this entry](#)

## [Wired on What’s Next Post-Verizon](#) [2:04 pm]

[Battle Not Over for File Sharers](#) – largely a rehash of recent discussions, but a few additions to be found in terms of legal strategies:

Last week's court decision preventing the recording industry from forcing Internet service providers to identify their subscribers on peer-to-peer networks offers new hope to file traders who have been sued.

But fighting the RIAA may prove costly for anyone hoping to challenge the trade group, which spends an estimated \$17 million annually in legal fees.

[permalink to just this entry](#)

## [Doug Isenberg's Internet Law Roundup](#) [2:01 pm]

From CNet News, a roundup of the year's Internet law developments: [Unexpected twists in Internet law](#)

Internet law in 2003 was full of surprises, with Congress passing an antispam bill, the courts blessing pop-up advertising, the music industry losing lawsuits and the Supreme Court finally upholding an Internet law.

Note that Doug runs [GigaLaw](#)

Update: Slashdot discussion, [The Year In Tech Law](#)

[permalink to just this entry](#)

## [This Should Be Interesting](#) [12:20 pm]

[Copyright, Innovation, and the Internet](#) at New York Law School. Check out the assignment list – [via [Derek](#)]

[permalink to just this entry](#)

## [Seem Linus Torvalds Disagrees With SCO, Again](#) [9:16 am]

Slashdot: [Linus Blasts SCO's Header Claims](#), citing a [Torvalds comment](#) to the kernel mailing list.

What this tells me is that the original code never came from UNIX, but some architectures later were made to use the same values as UNIX for binary compatibility (I know this is true for alpha, for example: being compatible with OSF/1 was one of my very early goals in that port).

In other words, I think we can totally demolish the SCO claim that these 65 files were somehow “copied”. They clearly are not.

Which should come as no surprise to people. But I think it's nice to see just how clearly we can show that SCO is - yet again - totally incorrect.

Update: See also the NYTimes [Creator of Linux Defends Its Originality](#) and a GrokLaw commentary: [Funniest Story of the Day: SCO's Linux “Expert” Contradicts Linus](#) (Semi-related: [Novell Registers Unix Copyrights](#))

[permalink to just this entry](#)

## [Billboard on the Verizon Decision](#) [9:00 am]

[RIAA: Suits To Continue Despite Verizon Court Win](#)

The Recording Industry Association of America expressed disappointment Friday after a federal appeals court ruled that the trade group has no authority to compel Internet service providers to turn over the identities of subscribers who use peer-to-peer file-sharing services. However, the trade group vowed to continue with its lawsuits against consumers suspected of infringing copyrights.

[...] The RIAA says it will now have to file “John Doe” lawsuits based on e-mail addresses of suspected infringers, a much slower process that requires significant judicial oversight.

[permalink to just this entry](#)

## [More on Corporate Sponsorship of Free Music Online](#) [8:55 am]

From CNN: [2004 to bring loads of ‘free’ Net music](#)

The great digital music giveaway is about to begin. In the new year, some of the world’s biggest brands will promote their products and services by doling out millions of free downloads through alliances with digital music services.

p>

“You’re going to see lots of free music given out via third-party companies,” buymusic.com founder Scott Blum says. “It’s not going to be Apple and iTunes driving the business. It’s going to be companies like Pepsi and other third parties that are promoting digital music on bottle caps and on labels.”

[...] The promotions come at a time when brand marketers, particularly beverage companies, are looking to establish broad connections between music and their products – a strategy well-served by digital music giveaways.

Music giveaways are understood to foster customer loyalty. What’s more, they provide consumers with powerful incentives to use the related products, executives say.

The trend has major implications for the nascent digital music business.

Digital download giveaways are just the latest wrinkle in a deepening relationship between the brand marketing community and the music industry.

Youth-oriented lifestyle brands like to piggyback on the strong emotional ties that young consumers have with their favorite songs and artists.

[permalink to just this entry](#)

## [A Look at a Related Internet Privacy Case](#) [8:43 am]

*The Register* has a *Security Focus* article by Mark Rasch: [Jane Doe ruling limits effect of RIAA legal defeat](#), discussing the implications of a Connecticut Superior Court decision that, he argues, may lead to a revised RIAA subpoena strategy that is equally intrusive/pervasive (of course, so far it’s only a Connecticut state court opinion, subject to review):

This provides a road map to the RIAA. While (absent a successful appeal) they may no longer issue hundreds of blanket DMCA subpoenas - at least in the District of Columbia - they can file hundreds of blanket ‘John Doe’ copyright infringement lawsuits and then issue hundreds of ordinary civil subpoenas. Or, they can go to Congress and have the DMCA amended to specifically include P2P networks.

So while the court ruling may slow the RIAA, there are many other arrows in their quiver.

Also, since the Connecticut case was about defamatory speech, rather than copyright infringement, I’m unconvinced of this argument – but there’s no question that the RIAA is not going to give up and go away...

[permalink to just this entry](#)

## Monday, December 22

### [Update on SCO Letters](#) [2:38 pm]

Slashdot has a bunch of pointers in [SCO Invokes DMCA, Names Headers, Novell Steps In](#), including:

- [the text of the letter](#) and
- a GrokLaw article on [Novell's copyright claims](#)

As Slashdot notes, the letter essentially asserts SCO's ownership of a bunch of header files (e.g., ctype.h) — interesting to claim what I assume is part of the ANSI and ISO spec for C/C++.

See also: [SCO sees loss on legal fees](#)

The Lindon, Utah-based company said it had a fourth-quarter net loss of \$1.6 million, or 12 cents per share, compared with a loss of \$2.7 million, or 26 cents per share, in the year-ago quarter. SCO said it would have reported earnings of \$7.4 million, or 44 cents per share, for the quarter before making a \$9 million payout to lawyers who represent the company in its Linux battles.

[permalink to just this entry](#)

## [BBSpot Reviews Online Music Stores – For Real](#) [11:43 am]

Not a joke: [Reviews: Digital Music Stores](#). The following emusic stores were reviewed:

- iTunes Music Store
- Napster
- Musicmatch
- Rhapsody
- Wal Mart
- BuyMusic
- EMusic

and this wrapup says it all:

### **The Perfect Service**

I think the perfect music program would have the selection, allowance feature and store design of iTunes, the abilities to download songs and playlist searching of Napster, the price of Wal Mart or BuyMusic's cheap tracks, the powerful jukebox, tagging features, and streaming service of Musicmatch, the file format and rights of EMusic, all fit into the program size of Rhapsody. As quickly as these programs are updating, maybe we'll get there some day.

(Orig timestamp – 8:52:03) Updated: See also Cory Doctorow's discussion with Fred von Lohmann about the Walmart system: [WalTunes ToS suck: they Own the music they sell you, not you](#). Also, Larry Lessig has his own analysis: [WalMart's way to the future](#)

Up-Update: Slashdot discussion – [Digital Music Stores Reviewed](#)

[permalink to just this entry](#)

## [Some Propaganda](#) [9:48 am]

'[Saving the Internet?](#)' purports to explain why the [recent Ninth Circuit decision](#) that found that internet over cable is a "telecommunications service" is a disaster for the industry. Of course, it fails to point out that, as things stand, cable companies can now monitor and control internet traffic over cable lines in ways that telephone companies cannot do with DSL service – but hey, you're supposed to buy the neo-con argument that all regulation is bad.

Truly dismal writing

[permalink to just this entry](#)

## [SCO's Last Gasp Strategy?](#) [9:35 am]

With their recent court loss, indicating that the SCO will have to demonstrate infringement in court soon, we get this move: [SCO Sends Second Warning Letter to Linux Users](#). Slashdot guesses this is a trick to distract the stock analysts ([SCO Gets More Desperate; Sends More Letters](#)) GrokLaw's just paying attention at this point in [More Threatening Letters from SCO](#) and [SCO Sends DMCA Notices](#),

[permalink to just this entry](#)

## [Surprise - LotR:TRotK is online](#) [9:28 am]

[Film Piracy Still Steals the Show](#) – so what's the MPAA response?

Like other blockbuster films, the copies of this movie appear to be high quality. The most popular versions seem to have been taken by professional pirates, rather than a regular ticket-buying audience member, he {Eric Garland of BigChampagne] said.

The Motion Picture Association of America, however, estimates that about 90 percent of films on peer-to-peer networks originated from camcorder versions of films, and is working to enact laws that will penalize those who surreptitiously record films in movie theaters.

Plus, there's the interesting question of economic harm given these kinds of results (from: ['Rings' Shows Trend Toward Global Premieres](#))

By opening in 28 countries in its first five days, "The Return of the King," made by New Line Cinema, raked in \$246 million — an astonishing sum, nearly a quarter of a billion dollars — from fans eager to revisit the world of hobbits and orcs.

Of course, there's the question of how global premieres are going to influence the use of region encoding of DVDs.

Instead the trend [of simultaneous global releases] is being pushed by the threat of movie piracy and the harsh realities of marketing costs, combined with ever-briefer theater stays as highly promoted films quickly saturate their markets.

As recently as three years ago Hollywood studios often released their biggest movies abroad only months after those films had opened in the United States, choosing release dates depending on what suited the local market.

Now they are finding they no longer have that luxury. When the first film of the "Rings" trilogy, "The Lord of the Rings: The Fellowship of the Ring," came out in 2001, New Line found pirated copies on the streets of Asian capitals within a day.

When "The Return of the King" opened around the world last Wednesday, there was no time for counterfeiters to compete with theaters. "We had not one pirated copy," said Rolf Mittweg, the studio's president of worldwide marketing and distribution. "Nothing surfaced before the film opened, which means we have done an extremely good security job. You definitely want to open around the world in as close proximity to the U.S. as possible, because of piracy."

[permalink to just this entry](#)

## [Another Holiday Gift - Johansen Acquitted](#) [9:08 am]

Via Slashdot: [DeCSS: Jon Johansen Acquitted In Retrial](#). From the cited news article: [DVD-Jon wins new legal victory](#)

Norway's most famous computer whiz got an early Christmas present on Monday. An appeals court in Oslo upheld Jon Lech Johansen's earlier acquittal on all counts of alleged copyright violations.

A verdict in the case, which has caught international attention, wasn't expected until early January. But the appeals court (*Borgarting lagmannsrett*) apparently didn't see any need to wait with its decision.

A panel of judges Monday cast aside the appeal that prosecutors had filed to a lower court decision handed down in January. That means the lower court's decision will stand, at least until another eventual appeal takes the case to Norway's supreme court.



[permalink to just this entry](#)

## [Real's Antitrust Complaint Against Microsoft](#) [9:06 am]

*The Register* offers up some interesting analysis, pointing out that this is about more than the desktop PC, but rather about the future of digital multimedia: [Why Real sued Microsoft](#)

According to records of a June 5, 1997 meeting made by Microsoft's Jim Durkin, at which Gates, Maritz and Muglia attended, Muglia said RealNetworks "is like Netscape, the only difference is we have a chance to start this battle earlier in the game". Adding to the familiarity, Real makes extensive use of the Findings of Fact in the earlier, federal suit against Microsoft.

"Microsoft's current tactics in digital media are the unlawful tactics it followed in annexing other markets: product bundling, technical tie-ins and/or lock-outs, restrictive licensing, exclusive dealing, predatory pricing, refusing to sell unbundled operating systems and discriminatory disclosure and withholding of information needed to interoperate with Microsoft's operating systems," claims Real.

"The prices at which Microsoft distributes its digital media products (zero and negative prices) are below any relevant measure of Microsoft's costs, including its average variable costs, its average total costs and its short-run and long-run marginal costs," Real argues.

[permalink to just this entry](#)

## Sunday, December 21

### [Today's Verizon v. RIAA Roundup](#) [7:13 pm]

- Mary Hodder: [Verizon Wins! Subpoenas Not Authorized](#)
- Derk Slater: [Verizon Wins](#)
- CNet's John Borland: [Is the RIAA out of the ballgame?](#)
- InfoWorld: [Update: Judge rules RIAA can't subpoena file-trader information](#)
- Wired News running the APWire: [Song Swappers Win a Big One](#)
- NYTimes: [Court Limits Efforts to Unmask Music Swappers](#)

The recording industry must first ask a judge before forcing Internet companies to disclose the names of people who trade music online, a federal appeals court in Washington ruled yesterday.

The sharply worded ruling, which underscored the role of judges in protecting privacy and civil rights, is a major setback to the record companies in their efforts to stamp out the sharing of copyrighted songs through the Internet. It overturns a decision in a federal district court that allowed the music industry to force the disclosure of individuals simply by submitting subpoenas to a court clerk without winning a judge's approval.

- LawMeme: [DMCA Does Not Require ISPs to Turn Over Names](#)

[permalink to just this entry](#)

### [Home-made, Idiosyncratic DVDs of TV Shows](#) [6:56 pm]

From the NYTimes - [A DVD Face-Off Between the Official and the Homemade](#) – something we won't get to see once the broadcast flag

hits our hardware.....

In the nostalgic memories of the Internet fan base, “Firefly” quickly became that sentimental fetish object: the brilliant series cut down before its time. A Web site called [Fireflyfans.net](http://Fireflyfans.net) continued to thrive; episodes were passed around via file-sharing programs. And this posthumous fan base waited expectantly for the show’s vindication: what has become television’s afterlife, the collectible DVD. Just in time for Christmas, that package finally arrives, a complete “Firefly” boxed set with all the goodies: three episodes never shown on network television, plenty of juicy extras, a melancholic mini-documentary on the show’s production, and commentary tracks by the show’s creators, its cast, even its costume designer — a permanent record of a series that once would have dissolved into network history.

But for the true completist, there’s another option out there: a handmade DVD created by Philip B. Gaines, a graduate student in digital media at the University of Washington. On this small, white two-disc set, Mr. Gaines puts forth his own idiosyncratic take on “Firefly,” scrolled over montages of stills and short excerpted scenes. His production includes episode summaries and visual mini-essays on subjects like “irony” and “violence.” He timed his project to piggyback on the official “Firefly” DVD (released by 20th Century Fox Home Video), touting his production on the geek-news site Slashdot.com. His discs are a charmingly ungainly valentine to the show — more experiment than true collectible. But they do offer a glimpse of a new possibility, the fan’s-eye approach to the television DVD.

[...] Movie geeks have already begun producing such tracks, ever since the film critic Roger Ebert’s rabble-rousing column on the subject for the online magazine YahooLife.com in February 2002. “I’d love to hear a commentary track by someone who hates a movie, ripping it to shreds,” Mr. Ebert wrote. “Or a track by an expert who disagrees with the facts in a film. Or a track by someone with a moral or philosophical argument to make. Or even a Wayne’s World-style track from dudes down in the basement who think ‘The Mummy Returns’ is way cool.” Mr. Ebert suggested that interested fans simply record their own tracks on MP3’s and post them on the Internet — legally providing alternate soundtracks for existing DVD’s.

[...] As for Mr. Gaines, he imagines his small “Firefly” set as a kind of first entry in an enormous future library — a future, he speculates, in which fans will act more like scholars. True enthusiasts will collect a whole library of DVD’s, he suggests: the official version, one or two commentary tracks by critics, and a selection by a particularly entertaining set of fans. How would such projects support themselves? Here, Mr. Gaines begins to verge into science fiction territory: someday, he suggests, interested patrons might offer to finance particularly excellent DVD commentators. “I worship art, almost literally,” he explained cheerfully. “You know, I want to sit there and talk about it. A great show like ‘Firefly’ just seemed like a perfect match to me: it deserves this kind of treatment.”

Update: (12/23) see Mary’s writeup - [Homemade DVD vs. Official Release](#)

[permalink to just this entry](#)

## [Napster Runs for President in ‘04](#) [6:48 pm]

That’s the title of a [Frank Rich piece](#) in today’s NYTimes discussing the Dean campaign. His essential point is that the record industry missed (and continue to miss, IMHO) the point of the Internet, and their businesses have suffered. The parallels with the conventional political establishment are easy to make, given Dean’s rise over the last six months.

I am not a partisan of Dr. Dean or any other Democratic candidate. I don’t know what will happen on Election Day 2004. But I do know this: the rise of Howard Dean is not your typical political Cinderella story. The constant comparisons made between him and George McGovern and Barry Goldwater — each of whom rode a wave of anger within his party to his doomed nomination — are facile. [...] This litany of flaws has been repeated at every juncture of the campaign this far, just as it is now. And yet the guy keeps coming back, surprising those in Washington and his own party who misunderstand the phenomenon and dismiss him.

The elusive piece of this phenomenon is cultural: the Internet. Rather than compare Dr. Dean to McGovern or Goldwater, it may make more sense to recall Franklin Roosevelt and John Kennedy. It was not until F.D.R.’s fireside chats on radio in 1933 that a medium in mass use for years became a political force. J.F.K. did the same for television, not only by vanquishing the camera-challenged Richard Nixon during the 1960 debates but by replacing the Eisenhower White House’s prerecorded TV news conferences (which could be cleaned up with editing) with live broadcasts. Until Kennedy proved otherwise, most of Washington’s wise men thought, as The New York Times columnist James Reston wrote in 1961, that a spontaneous televised press conference was “the goofiest idea since the Hula Hoop.”

Such has been much of the reaction to the Dean campaign's breakthrough use of its chosen medium. In Washington, the Internet is still seen mainly as a high-velocity disseminator of gossip (Drudge) and rabidly partisan sharpshooting by self-publishing excoriators of the left and right. [...]

For all sorts of real-world reasons, stretching from Baghdad to Wall Street, Mr. Bush could squish Dr. Dean like a bug next November. But just as anything can happen in politics, anything can happen on the Internet. The music industry thought tough talk, hard-knuckle litigation and lobbying Congress could stop the forces unleashed by Shawn Fanning, the teenager behind Napster. Today the record business is in meltdown, and more Americans use file-sharing software than voted for Mr. Bush in the last presidential election. The luckiest thing that could happen to the Dean campaign is that its opponents remain oblivious to recent digital history and keep focusing on analog analogies to McGovern and Goldwater instead.

[permalink to just this entry](#)

## Friday, December 19

### [CNet's Roundup of Today's Verizon Decision](#) [5:29 pm]

#### [Ruling sounds sour note for record industry](#)

- [Ruling rebuffs record industry effort](#)
- [Read the court's decision](#)
- [What the ruling means for file swappers](#)
- [Dutch court nixes bid to control Kazaa](#)

[permalink to just this entry](#)

### [Followup to the Verizon Decision](#) [5:22 pm]

#### [Dutch Court Throws Out Attempt to Control Kazaa](#)

*by Marcel Michelson and Bernhard Warner*

AMSTERDAM/LONDON (Reuters) - The Dutch supreme court on Friday threw out an attempt by a music copyright agency to put controls on popular Internet file-swapping software system Kazaa, a ruling the music industry attacked as flawed.

The decision is a fresh blow to the media industry, which has fought to shut down file-sharing networks they say have created a massive black-market trade in free music, films and video games on the Internet.

"The victory by Kazaa creates an important precedent for the legality of peer-to-peer software, both in the European Union (news - web sites) as elsewhere," Kazaa's lawyers Bird & Bird said in a statement.

The decision by the Dutch court, the highest European body yet to rule on file-sharing software, means that the developers of the software cannot be held liable for how individuals use it. It does not address issues over individuals' use of such networks.

The International Federation of the Phonographic Industry (IFPI), the music trade group representing independent and major music labels including Warner Music, Sony Music, BMG, EMI and Universal Music, criticized the ruling as "one-sided" and vowed to continue its legal crusade elsewhere.

[permalink to just this entry](#)

### [Here We Go Again](#) [5:17 pm]

This fight has been brewing for a while – it didn't work for Netscape, but this time around there are others with stakes in this one's outcome: [RealNetworks Accuses Microsoft of Restricting Competition](#)

In a 65-page complaint filed in Federal Court in San Jose, Calif., RealNetworks, a maker of software for playing digital audio and video content, argues that Microsoft has unfairly damaged its business by linking Windows Media Player to the Windows operating system.

“We believe that our business would be substantially larger today if Microsoft were playing by the rules,” said Rob Glaser, chief executive of RealNetworks, which is based in Seattle.

[...] “In a sense this is the next chapter following on the heels of the Netscape issue,” said Andrew I. Gavil, a law professor at Howard University in Washington. “In some ways, it's become even more significant because of the expansion of the digital content issue.”

See also Wired News' AP wire feed: [RealNetworks: MS Won't Play Fair](#); also SFGates' [RealNetworks sues Microsoft on antitrust: Music player firm says software giant hasn't made good on pact](#)

[permalink to just this entry](#)

[Woo-hoo!](#) [1:45 pm]

Nothing like being in meetings and missing all the news!! Donna's e-mail to me describes it as a holiday present, and I have to admit that it gives me that sort of pleasure. (still reading – updates to come)

- [No. 03-7015; Recording Industry Association of America, Inc. Appellee v. Verizon Internet Services, Inc., Appellant](#)

On appeal Verizon presents three alternative arguments for reversing the orders of the district court: (1) § 512(h) does not authorize the issuance of a subpoena to an ISP acting solely as a conduit for communications the content of which is determined by others; if the statute does authorize such a subpoena, then the statute is unconstitutional because (2) the district court lacked Article III jurisdiction to issue a subpoena with no underlying "case or controversy" pending before the court; and (3) § 512(h) violates the First Amendment because it lacks sufficient safeguards to protect an internet user's ability to speak and to associate anonymously. **Because we agree with Verizon's interpretation of the statute, we reverse the orders of the district court enforcing the subpoenas and do not reach either of Verizon's constitutional arguments.** [slip op. 3] [emphasis added]

Plus, a look at the notion of "strict construction" when legislated rights are concerned – not to mention pointing the finger at the next battleground:

We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforeseen internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress; only the "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology." See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 431 (1984). [slip op. 15]

- CNet News: [Court: RIAA lawsuit strategy illegal](#)
- NYTimes: [Record Industry May Not Subpoena Online Providers](#)
- CopyFight: [Verizon Wins Victory for Privacy](#)
- Ernest Miller: [Verizon Wins Against DMCA Subpoenas](#)
- Slashdot: [Appeals Court Rules Against RIAA in DMCA Subpoena Case](#)

- The EFF's case archive: [RIAA v. Verizon](#)

[permalink to just this entry](#)

## Wednesday, December 17

### [MIT Hack - Wright Brothers At MIT](#) [12:12 pm]



Since we couldn't get to Kitty Hawk to celebrate the 100th anniversary of flight, the Wrights apparently came here to Cambridge instead. (MIT Physical plant, as you can see, is already working at getting it off the Engineering Library atop Building 10) See more images at the [MIT Hacks Page](#) as well as the [Image of the Day writeup](#)

[permalink to just this entry](#)

### [Philip's DRM](#) [8:53 am]

#### [No, Really, You Can't Copy These](#)

Philips Electronics said on Tuesday it was six months away from launching a system against illegal copying that will allow consumers to play digital video and music on any digital media player.

Philips hopes the so-called digital rights management (DRM) system being developed by Intertrust, which it jointly owns with Sony, will replace a confusing array of proprietary systems.

Slashdot discussion: [Intertrust Plans Universal DRM System](#)

## [Surprise! Copyright is Hard to Understand](#) [8:49 am]

From Wired News: [Film Fans Befuddled by Copyright](#) – more fuel for [Jessica Litman's](#) thesis that copyright has become too byzantine to be enforced in its current forms

A major studio's recent action to curtail online sales of its films has left some movie buffs confused about where and when purchasing foreign DVDs is legitimate.

In general, U.S. law permits consumers to buy imported DVDs for personal use. But the law is a little murkier for retailers.

[...] So when and where can film purists seek out the original versions of foreign movies?

In the non-Internet world, if one buys a foreign DVD overseas and brings it home in a suitcase for personal use, that's legal. Hauling 100 DVDs back to the United States and selling them, however, is not.

Ordering a movie online from an overseas distributor, so long as it is not a counterfeit copy, is also permitted under U.S. law.

[...] But one industry attorney argued that finer points regarding the legalities of buying online from foreign sites have yet to be decided by courts.

"I think if you buy one copy over the Internet for your personal use, it's unclear right now where that would fall," said George Borkowski, an attorney with Mitchell Silberberg & Knupp. "I don't think the law has been resolved specifically on Internet purchases."

A followup to [Logical Extension of the 2600 Decision?](#)

[permalink to just this entry](#)

## [John Depp Keeps Filing](#) [8:34 am]

### [Friends of Aimster back Supreme Court bid](#)

The American Association of Physicians and Surgeons (AAPS), Privacy Innovations Inc., and online author and librarian Eric Flint have all voiced their support for the Aimster/Madster peer-to-peer service, which is currently in limbo after a lower court shut it down. John Depp, Aimster's creator, is awaiting word from the Supreme Court as to whether or not it will hear the case and examine whether the injunction should be repealed. In their letters to the court, the Aimster backers argue that shutting down an encrypted peer-to-peer file swapping service impedes free speech rights and damages the potential of a new technology before it has time to play out.

[permalink to just this entry](#)

## [Ubersoft and DRM](#) [7:53 am]

[Dec 17 Ubersoft comic](#) – DRM and wordprocessing software

[permalink to just this entry](#)

## Monday, December 15

### [Microsoft and Lock-In](#) [11:19 am]

An entertaining assessment of current Microsoft moves over at eWeek: [No More Microsoft Support For You](#)

It will be two days before Christmas, and all through the world, not a creature will be stirring except Microsoft employees taking many programs off the Microsoft sales racks.

[...] What Microsoft is really doing is forcing business customers to upgrade their operating systems to XP and Server 2003 and their application suites to Office XP and Office 2003. I think the company is doing this to kick up corporate XP sales. (Both Server 2003 and Office 2003 have had disappointing sales.)

In a way, I can't blame Microsoft for this move. As IDC's Kusnetzky told me, Microsoft has already supported its programs long after most companies would have pulled the plug.

[...] Worse still, if you take a close look at Microsoft's current generation of software, you'll quickly see that it's all designed to lock you into Microsoft products, from your desktop to your server.

Take, for example, Office 2003. Unless you use its groupware and presence functionality, it's really little more than a cosmetic improvement over Office XP. To use those new tools, though, you need to upgrade your server to W2K or Server 2003 so you can run Exchange 2003, SharePoint Portal Server 2003 and Live Communications Server 2003. Oh, and if you haven't moved from domains to Active Directory, you'll need to do that, too.

[...] From where I sit, Microsoft is not only bullying customers into upgrading, it's making it so pricey to do so that even people who love Microsoft must start thinking about alternatives.

[permalink to just this entry](#)

## [Speaking of Internet Policy](#) [8:54 am]

### [Phone Service Over Internet Revives Talk of Regulation](#)

In an interview on Thursday, Michael K. Powell, the chairman of the F.C.C., said he had not made up his mind on that question. But he was not at all shy about stating his preliminary view - that Internet-based calls are fundamentally different from traditional phone calls and ought to be regulated cautiously, if at all.

Mr. Powell noted that while Internet-based calls might serve the same function as calls over conventional phone lines, the underlying technology was different enough that it would not make sense to subject them to "100 years of judgments" and regulations. "Let's get this thing right and define it as truer to its real nature," he said, referring to the new technology.

His views are far from universally supported, given the many complex political and financial interests at stake.

What is clear is that the existing telephone infrastructure is heavily regulated, on both the state and federal levels, with intricate rules intended to keep phone access universally accessible and affordable.

Gene Kimmelman, the senior director for public policy at Consumers Union, said those regulations existed to satisfy important public policy concerns. He contended that goals like universal access would be gravely threatened if the world went to Internet-based services that were unregulated.

[permalink to just this entry](#)

## [A Look At Internet Policy](#) [8:51 am]

### [No recovery for the Internet](#)

The Internet industry, which once led the economy and set new levels of productivity for the nation, is stagnant. The stagnation is due primarily to the incoherent, conflicting and threatening policies of the federal government.

At the Federal Communications Commission, regulators are still whimsically pretending that broadband carried over a cable company's copper wire should be treated differently than broadband carried over a telephone company's copper wire. Wireless Internet is barely considered at all; satellite Internet is ignored; and policies that could spur investment in voice over Internet Protocol may finally get some consideration—next year.

Internet policy is an even bigger mess in Congress. After years of concerted effort, there is still no national policy for the release of broadband or for the protection of private information on the Internet. Efforts to cut away unnecessary regulation and spur investment are hopelessly stalled. The U.S. Congress cannot even—after five years of flailing—manage to pass a federal law to make spam illegal.

[permalink to just this entry](#)

## [Logical Extension of the 2600 Decision?](#) [8:38 am]

From Wired news: [Studio Warns Kung Fu Site](#)

For the past three years, Mark Pollard has been writing reviews and posting news on his website Kung Fu Cinema.

But while he's used to feedback from fellow fans of Kung Fu movies, Pollard was caught by surprise recently when he heard from a new correspondent – Miramax Film Corporation. In a letter drafted by its legal affairs department, the studio demanded that Pollard stop selling copies of a Chinese film for which it owns the distribution rights.

Pollard said he found the letter particularly shocking given that Kung Fu Cinema does not sell films. It merely links to websites that do.

“It's pretty hard-core as far as I'm concerned,” said Pollard, a Seattle bookstore employee. “I don't sell anything except my Kung Fu Cinema T-shirts.”

[...] Nonetheless, Miramax contends that its decision to send a cease-and-desist letter to the Kung Fu Cinema site was a sound one.

“The letter served its purpose because Mr. Pollard stopped linking to the sites,” said Matthew Hiltzik, a representative for Miramax. “By removing these links, he's making it more difficult for people to purchase these films, thereby allowing us to protect our interest in these properties.”

Update (5:40PM): Slashdot discussion – [Miramax C&Ds Kung Fu Movie Reviewer](#)

[permalink to just this entry](#)

## [A Bet That Methods for Online Music Selling Is Established](#) [8:22 am]

CNet News reports that Loudeye is going to announce the availability of a set of software tools that will allow buyer to set up their own online music stores: [Loudeye builds off-the-shelf music store](#). What's particularly interesting about this article is the implicit assumption that **online music distribution is not about profit, but about cross-promotion** – another indication of a return to sponsorship (corporate, in this case) as a basis for music development.

Under the program, Loudeye will work with Microsoft to handle the infrastructure and distribution for online music services branded by other companies looking to sell songs online or to enter the digital media business in some other way. Early customers of the service include AT&T Wireless and Gibson Audio, a division of Gibson Guitars.

[...] However, the profit potential for these services remains dim. Apple has stated that it does not make money from iTunes, relying instead on the service's ability to drive demand for its iPod digital music player. Other industry executives have said that profits are possible, even if they are razor-thin.

Loudeye's Cavins said there is room for an intermediary in the business despite the tiny profit margins. His company is looking for customers who are interested in digital music distribution as a promotional tool for another product or service, rather than as a standalone business, he said.

“There are a lot of companies that are not your usual suspects that will pay to have services that will drive cross promotion,” Cavins said. “What it comes down to is that there are companies that are learning that using digital media is a good way to cement a brand.”

[permalink to just this entry](#)



## [Upcoming Metallica Documentary](#) [8:15 am]

From Billboard, a discussion of the upcoming "Metallica: Some Kind of Monster" – [Metallica Film Filled With 'Monster' Revelations](#)

An unflinching, warts-and-all look at the band, the film will be part of the 2004 Sundance Film Festival and will be released next year in theaters.

[...] Struggles with artistic credibility, the Napster controversy and accusations of "selling out" are presented for all to see. In one scene, manager Cliff Burnstein pressures the band to record promotional announcements for an unnamed radio conglomerate's contest. When Burnstein explains that the company may retaliate by trying to ruin the band's career, Hetfield's anger and surprise inspires him to write the lyrics, "Wash your back so you won't stab mine" for the "St. Anger" track "Sweet Amber."

[permalink to just this entry](#)

## [Roland Backs Down?](#) [8:08 am]

Slashdot reports that Roland has backed down on claiming copyright to elements of the [Roland MT-32 emulation project: Roland Backs Down On MT-32 Emulator](#). Interestingly, although the [EFF](#) is credited with helping to bring this about, I cannot find any resources on their site.

From the Furdlog archives, [A Few More Slashdot Tales](#) and [LawMeme on the Roland MT Discussion](#)

[permalink to just this entry](#)

## [BBSpot Humor](#) [7:54 am]

### [God Considers Smiting Bible Pirates](#)

God did not rule out smiting as a final measure against those who share his most famous work, the Bible, on the Internet. This marks the first time a deity has spoken on IT-related questions since Steve Jobs was temporarily Enlightened when touching the One True iMac some years ago.

[...] Since large portions of the Bible are many centuries old, many people believe the work to be in the public domain. Not so, said God. "Look, most copyright laws are based on something like the author's lifetime plus, let's say, 15 years. News flash: I'm still here."

"I am a jealous God," He said, "but I am by no means unreasonable. If the person will stop distributing My copyrighted materials, there will be no further consequences. Like I've said before: hate pirating, love the pirate."

Ironically, some of those most likely to be hit by these measures are among God's biggest fans. The Reverend Alfred Jackson is a minister at the church of St. Cecilia in Kansas City. In his spare time, he maintains the Bible study website "eChapter and eVerse," which cross-references large parts of the bible with commentary from clergy and laypeople from around the world.

[...] Jackson said he had had several emails from someone claiming to be the Deity, but had first dismissed them as pranks. When he received the second 'cease and desist', Jackson contacted the EFF and asked for advice.

Marie Dang, an attorney with EFF said smiting was clearly an unreasonable response to alleged copyright infringement. "I realize that legal text often spells out all the details and ramifications right from the start. But mentions of smiting and damnation are hardly suitable for a first letter," said Dang.

[...] When asked what His next step might be, God was reluctant to discuss specifics. He stressed that He would consider the effect of His actions on the meek. "Let's make one thing clear," He said, "I may be omnipotent, but I'm not crazy: It's not like I think I'm Jack Valenti."

## [New Get Your War On Cartoon Set](#) [7:47 am]

I missed the release of [a new page](#) of [Get Your War On comics](#). In the face of all the rhetoric over the past few days, I found [this one particularly on point](#), although you can see that David Rees [works on Sundays](#).

Update: Unsurprisingly, Iliad of [UserFriendly was hard at work](#), too.

[permalink to just this entry](#)

## Sunday, December 14

### [Let's Definitely Let WSIS Run Things](#) [11:37 am]

They've already mastered the use of the RFID tag: [Bug devices track officials at summit](#) [pdf]

Officials who attended a world Internet and technology summit in Switzerland last week were unknowingly bugged, said researchers who attended the forum.

Badges assigned to attendees of the World Summit on the Information Society were affixed with radio-frequency identification chips (RFIDs), said Alberto Escudero-Pascual, Stephane Koch and George Danezis in a report issued after the conference ended Friday in Geneva. The badges were handed out to more than 50 prime ministers, presidents and other high-level officials from 174 countries, including the United States.

The trio's report said they were able to obtain the official badges with fraudulent identification only to be stunned when they found RFID chips — a contentious issue among privacy advocates in the United States and Europe — embedded in the tags.

Possibly not that earth-shattering, but an interesting demonstration of just how far this technology has already gone, as well as the implicit privacy questions.

Slashdot discussion: [Officials secretly RFID'd at Internet Summit](#) – plus this earlier discussion [WSIS Physical Security Cracked](#)

[permalink to just this entry](#)

### [Two More Articles on the Canadian Copyright Ruling](#) [10:53 am]

- NYTimes – [Canadian Ruling on Web Music](#)
- CNet - the source for the NYTimes article; at least CNet gets the title right - [Canada deems P2P downloading legal](#)
- 
- Another one - *The Register*: [Canada OKs P2P music downloads](#)

[permalink to just this entry](#)

### [A Couple of NYTimes Pieces on the Practicalities of Copyright](#) [10:46 am]

- [Letting 'Let It Be' Be: McCartney Wins](#) – when the artist wants to remake his own recordings

[Y]ou might have some uneasiness about how mutable music is becoming. With technology making after-the-fact alterations easier and the record companies eager for sure sellers, it might one day be practical for artists to rework releases the way playwrights alter scripts between engagements? Shania Twain's latest album, "Up!," is sold as a two-disc set of country and rock takes on the same songs (in Europe, it's a two-disc set of rock and rhythmic pop). What's to prevent a band from releasing a live album with stage patter appropriate for each city ("What's up,

Brooklyn,” for New York; “Hello, Cleveland,” for Ohio). For that matter, who’s to say a change has to be artistic in nature: why settle for kicking the drummer out of the band when you can go back and remove his performances from previous albums?

Music is made in the studio, but it accrues meaning over time. We hear songs the way we’ve learned to hear them. Think of the way the sweeping orchestration of “The Long and Winding Road” made the song a bittersweet valediction for the Beatles. Thanks to “Let It Be . . . Naked” we all know that was edited in: the band never intended to express any such emotion in that way. Now, though, after listening to it for 30 years, it certainly seems like they did.

- [Greatest DVD’s Never Made: A Most Wanted List](#)

Sometimes, ownership is in dispute. Last February, a new video company, Koch-Lorber, announced that one of its first DVD’s would be “La Dolce Vita” by Fellini. The company had bought the rights from a small company called International Media Films, which claimed it owned the movie.

But Paramount Pictures claims that it owns “La Dolce Vita.” A legal battle is brewing. Koch-Lorber’s DVD has been delayed. Paramount, meanwhile, is reportedly preparing its own DVD.

Other films are simply being withheld. None of Harold Lloyd’s silent comedies are on DVD, for example, because Lloyd’s granddaughter, who owns them, won’t lease or sell the rights.

The avidly awaited, definitive version of Ridley Scott’s science-fiction classic, “Blade Runner,” won’t be out on DVD anytime soon for stranger reasons.

When “Blade Runner” was being shot in the early 1980’s, Bud Yorkin, a veteran television comedy producer, and Jerry Perenchio, now the C.E.O. of Univision, were the film’s bond-completion guarantors. When the film went over budget, by contract they assumed ownership of the film. Paul Sammon wrote in his book “Future Noir: The Making of ‘Blade Runner’ ” that they hated the film, had bitter disputes with Mr. Scott and tried to take it away from him altogether.

[...] Three years ago, Mr. Scott announced that he was working on a three-disc box set, which would offer all the versions of the film, including a new and polished director’s cut with previously unseen footage and scads of bonus features. Then, at the end of 2001, Warner Brothers, which was planning to distribute the discs, pulled the plug. It did so, according to a producer who worked on the project, because Mr. Perenchio gave no sign that he would let them be released.

Mr. Perenchio, speaking through an assistant, had no comment on the situation. (Warner Brothers still sells the 1992 “director’s cut,” though the picture quality is mediocre.)

- [The Evolution of a Daffy Species](#) – on the Looney Tunes Golden Collection DVD release

Perhaps because the rights to the films are spread among different divisions of the Time Warner empire — or perhaps because Warner Home Video didn’t want to risk confusing home consumers with strange, black-and-white cartoons — the “Golden Collection” concentrates on films made after 1948.

[permalink to just this entry](#)

## [The Year in Ideas – Darknets](#) [10:32 am]

From the NYTimes Magazine Section, and their year in ideas: [Darknets](#)

Darknets

By GARY RIVLIN

Published: December 14, 2003

When the U.S. military sought to create a secure network over which soldiers in Tikrit could share intelligence on medical

supplies and road conditions with nongovernmental organizations in New York and Geneva, it turned to a software package called the Groove Workspace. Using Groove, Central Command set up a so-called Darknet. Darknets allow a group to create a digital utopia that is equal parts socialist and elitist: participants can get information freely as long as they share the same software and have been granted the access code.

A Darknet isn't as much a new technology as an old idea – the corporate Intranet – reconstructed for a paranoid age. A Darknet offers all the security of a private in-house network, but it allows users to send encrypted messages and documents around the world through that vast, bustling, danger-filled wasteland of sprawl called the Internet. Sri Lankan human rights activists now trade cloaked electronic communications with one another using a Darknet, as do researchers at GlaxoSmithKline who work in geographically dispersed teams.

Darknets are suddenly au courant among the cybercool as well. This past summer, when, in a frenzy against music downloading, the Recording Industry Association of America started slapping suits on children and grandmothers, hundreds of thousands of music devotees flocked to Web sites like Bad Blue and Waste. Like Napster and KaZaA, these sites let users sift through the public contents of one another's hard drives and swap files on the Internet. But like the soldiers in Tikrit, file-swappers need an invitation to enter. Inside the velvet-roped cyberclub of the Darknet that Bad Blue or Waste creates, members can trade purloined music or movies or whatever it is they want to exchange, having been waved inside by the bouncers at the door.

[permalink to just this entry](#)

## Friday, December 12

### [The Matt Drudge of Alphaville](#) [4:55 pm]

Farhad Majoo tells a modern tale of woe: [Raking muck in "The Sims Online"](#)

In the real world, Peter Ludlow is an academic, a professor of philosophy and linguistics at the University of Michigan whose books go by sober titles like "Readings in the Philosophy of Language," and "Semantics, Tense and Time: An Essay in the Metaphysics of Natural Language." He's well-regarded in his field and engaging enough on the phone, but Ludlow is, even by his own admission, not a very interesting person. That is to say, Peter Ludlow is nothing like Urizenus, Ludlow's alter ego in the virtual world of "The Sims Online."

Urizenus is an unabashed muckraker. In the mold, perhaps, of Walter Winchell or Joseph Pulitzer, he investigates the shady underside of life in Alphaville, one of the game's largest cities, and posts all his sensational discoveries on the [Alphaville Herald](#), a blog that he describes as the only newspaper covering "The Sims Online." In the couple of months since the blog went live, Urizenus has interviewed many of Alphaville's most infamous scammers, thieves, money launderers, prostitutes (some of whom, he says, are minors) and other dubious types, and he's documented attempts by the community to create a kind of governing authority to police the place.

Urizenus and his compatriots at the Herald have also aimed their bullhorn at Maxis, the company that created "The Sims Online" and that runs the place; in blog entry after blog entry, the Herald describes Maxis as being signally indifferent to the needs of people who populate the game, and it documents the many reasons why "The Sims Online" – which was predicted to be a blockbuster and made the cover of Time magazine before its launch late in 2002 – has been a money-loser for Electronic Arts, Maxis' parent company.

But the Herald's relentless criticism does not appear to have gone down well at E.A. On Wednesday, in a move that Ludlow describes as arbitrary and capricious, E.A. terminated Urizenus' "Sims Online" account. "While we regret it," E.A. told him in a letter, "we feel it is necessary for the good of the game and its community." Alphaville's Citizen Kane was kicked out of town.

[...] "[These virtual worlds] are a strange sort of commercial space where communities come to exist, but there's a tension between the communities and the private commercial company," says Julian Dibbell, the author of "My Tiny Life," a kind of memoir about the virtual world LambdaMOO. "It's similar to what you have with shopping malls. They're becoming the last refuge of public space for teenagers, but they're run by companies, and they can kick you out on a whim."

The story also prompts a host of compelling questions regarding the nature of virtual existence. For instance, can something like prostitution occur online? And what about community-based policing – is that possible, or desirable, in the Sim world? And, finally, does E.A. have any obligation to allow a free press to document how all these issues will play out in "The

Sims Online”? After all, it’s their world – why can’t they run it how they please, however capricious their rule may seem to others?

See also Donna’s posting: [Gag Me With a TOS Agreement](#)

[permalink to just this entry](#)

## [Changerz – Another Experiment](#) [4:47 pm]

From MI2N: [A Reason To Pay For New Music: Fan Orders Can Now Launch Major New Artists Through Changerz](#). See their site: [Changerz](#) – their [tour](#) is a little more informative

We’re the first company to really turn the tables in music/entertainment. Instead of being told what you should like, you get to come together with thousands of other like-minded persons to jointly launch the next best bands, and participate in their success! It’s fun and you’ll be showing the big companies who’s boss, so what do you have to lose? Flex your muscle today!

[permalink to just this entry](#)

## [Webcaster Alliance and Hatch’s EnFORCE Act](#) [4:42 pm]

[Webcaster Alliance Blasts Proposed RIAA-Friendly Legislation](#) (see also [Webcast Alliance to fight expansion of RIAA antitrust exemption](#) )

The announcement is in response to Senate Judiciary Committee Chairman Orrin Hatch’s recent introduction of the Enhancing Federal Obscenity Reporting and Copyright Enforcement Act of 2003(the EnFORCE Act), a bill intended to expand the RIAA’s power by broadening the narrow antitrust exemption the RIAA currently enjoys. The EnFORCE Act would expand the existing exemption to cover all compulsory mechanical licenses under section 115 of the Copyright Act.

“A Federal Judge recently approved a \$143 million settlement in the CD price-fixing case that was brought against the RIAA’s Big 5 record label members,” Ann Gabriel, President of Webcaster Alliance said, “Yet here they are attaching additional language to expand their antitrust exemptions to a bill they know most legislators would have a hard time opposing, since it deals with the exploitation of children. This is so typical of the RIAA and their manipulative, smoke and mirrors tactics.”

[permalink to just this entry](#)

## [The Canadians Come Through for the CRIA ... \[updated\]](#) [3:43 pm]

And levy fees on MP3 players: from the Copyright Board’s [WWW site](#), [the decision](#) and the [press release](#).

From the [fact sheet](#):

### **What specific forms of blank recording media are subject to the levy?**

Analog Audio Cassette Tapes: ....

CD-R and CD-RW: ....

CD-R Audio and CD-RW Audio: ....

MiniDisc: ....

Non-Removable Memory Permanently Embedded in a Digital Audio Recorder: This covers two general types of memory embedded in digital audio recorders (such as MP3 players) capable of recording and playing back music files most commonly stored in MP3 format. The first category covers solid state memory, containing no moving parts. Typically this type of memory has between 32 and 256 Megabytes (Mbs) of storage capacity. The second category covers spinning hard-

disk drives that are technically similar to those found in personal computers. The capacity of these storage devices is much larger, ranging from 5 to over 200 Gigabytes (Gbs).

Yesterday's Slashdot discussion has been updated: [Canadians \[Will\] Pay Levy on MP3 Players - Updated](#)

See also CNet News' [Canada deems P2P downloading legal](#), but note that the title is surprisingly misleading for a supposed news organization - strictly speaking it should be "Canada deems that the '2P' part of P2P is legal."

In a ruling released Friday, copyright regulators in Canada said downloading copyrighted music from peer-to-peer networks appears to be legal under Canadian law but that uploading is still prohibited.

[permalink to just this entry](#)

## [Some Arts/Rights News](#) [3:40 pm]

- ['Will & Grace' Creators Sue Over Rights](#)

The mergers of networks and production companies in the 1990's have led, as the current lawsuit pointed out, to the "increasingly common case of negotiations between closely related or commonly owned parties." The result is that profit participants in hit television series, which can earn tens of millions of dollars, sometimes assert that negotiations are designed in large measure to benefit the parent company.

- [Progress Made on BMG-Sony Music Merger](#)

[permalink to just this entry](#)

## [More Content Reference Forum](#) [3:35 pm]

I've been adding too much to [yesterday's posting](#), so here's a placeholder for more on the idea today

- Wired News regurgitation of a Reuters Newswire: [Reaping Profit From Peer-to-Peer](#)
- Slashdot's weak discussion: [Music Industry Develops Centralized File-Sharing System](#)

[permalink to just this entry](#)

## [Distaff](#) [9:23 am]

Ernest asks me why [I characterized his posting](#) "of or relating to women or women's work." (A distaff is the stick upon which the products of spinning are held.) I suppose I made a somewhat too substantial a leap in the figurative sense. My general experience with the word has to do with [genealogy](#), where it means the [woman's side of the family](#), and from some (mis?)readings where there is an implication that the "distaff side" is related, but not necessarily on the mainstream - for example, the idea that, in royal families, cousins on the distaff side are not really terribly interesting when it comes to figuring out who's in line for the throne. And odd thought, since of course, royalty had all sorts of terribly unattractive mechanisms in place to ensure that babies were not switched at birth.

Unfortunately, I kept track of the "related but not necessarily on the main stream" thought without remembering the formal definition of the word (see [OED.com](#), for example), so I am sure that I have offended some with the apparent connection between "distaff" and pornography. Please accept my apologies.

[permalink to just this entry](#)

## Thursday, December 11

### [Speaking of Convenient...](#) [7:19 pm]

See this Slashdot discussion: [Police and Lawyers Love E-ZPass](#) (Referring to this article: [Electronic Toll Records Help Solve Crime \[pdf\]](#))

[permalink to just this entry](#)

## [Content Reference Forum](#) [7:04 pm]

Pursuant to [my meager followup](#) to the compulsory licensing discussion that Ed Felten has started (see Ernest's [distaff related, albeit on a different tack, discussion](#)), I saw this news piece ([Tech Group Aims at Profit-Friendly File-Sharing—pdf](#)) about the [Content Reference Forum](#).

The world's largest software and music companies, together with a broad alliance of companies, on Wednesday said they would work together in a bid to transform Internet file sharing from a haven for piracy into a potential profit center.

[...] The group on Wednesday issued an initial set of technology specifications in a bid to create a system in which users would share customized Internet links, called "content references," instead of swapping song or film files directly.

[...] For example, if a user wanted a song in an MP3 format from a friend who has it in a different file format, the links would serve as a sort of middleman that would help locate that specific content in the appropriate form.

How *convenient* – read this description from the CRF's WWW page:

At the crux of The Content Reference Forum's architecture are "Content References," data packages that uniquely identify content and the context in which it will be used. Content References are resolved by "Reference Services" that determine the right content, user context (including rendering environment, language and location) and commercial terms of usage. The "Reference Service" facilitates the seamless acquisition of appropriate content (e.g., matching consumer's preferences and platform capabilities) by providing an offer or offers for the consumer to buy the content, or connecting the consumer to the appropriate retail source, per contractual agreements for content distribution.

A real world example of a Content Reference is when a consumer wishes to share a video file with a friend. Via the consumer's personal computer, she sends the friend a "Content Reference" - a pointer describing the content and the prior value chain participation (e.g., an original retailer). When the friend clicks on the reference, her computer messages a "Reference Service" with another "Content Reference" which unites the information about the content and its distribution parameters with the information supplied by the friend (e.g. her country, preferred device and format). The "Reference Service" checks this information against contractual agreements contained in the Reference Service, and presents a set of purchase or promotional offers to the friend. This is all done transparently to both consumers.

Now, ask yourself – this certainly is a workable system, and you certainly could layer compulsory licensing mechanisms onto it – but would you want to participate? Would it matter who ran it? Would you trust them? And, if you didn't want to use this system, how would you react when it is made compulsory? (see Steven Levy's writeup [below](#))

Update: See Mary Hodder's comments: [New Music Model Proposed by Vivendi and MS](#), starting with this LA Times article – [A Toll Booth for File Sharers \[pdf\]](#)

Up-update: Now Derek's included a bit more: [New/Old Music, DRM, & P2P Model](#)

Re-up-update: Slashdot seems to miss the point: [Music Industry Develops Centralized File-Sharing System](#)

[permalink to just this entry](#)

## [Acacia Research and IP Failure](#) [6:00 pm]

From the Washington Post: [Patenting Air or Protecting Property? \[pdf\]](#)

Acacia Research Corp. started by targeting dozens of adult entertainment companies, demanding royalties of as much as 4 percent of their revenue from audio and video streaming. Now the firm is seeking fees from universities that use Web video for remote learning, from companies that serve up movies to hotel rooms, from cable and satellite providers, and from

major streaming-media companies such as RealNetworks Inc. and America Online Inc.

“It’s pretty much the sky’s the limit as to where the impact might fall,” said a chagrined John H. Payne, director of educational technologies at the University of Virginia’s division of continuing education, which uses online video for lectures and courses. “It’s like patenting air.”

The Acacia case highlights why a growing chorus of corporate and government officials is warning that the U.S. patent system is broken, threatening to stunt technological innovation.

They argue that an overwhelmed U.S. Patent and Trademark Office is simply approving too many dubious and overly broad patents, especially in the software and Internet realms.

The potential result: a digital world carved up into so many pieces that it loses its power to easily link people, communities and ideas.

The country “needs to revamp not just the patent system, but the entire system of intellectual property law,” said Andrew S. Grove, chairman of Intel Corp. “It needs to redefine it for an era that is the information age as compared to the industrial age.”

Slashdot discussion: [When Good Patents Go Bad](#)

[permalink to just this entry](#)

[I've Been Busy....](#) [1:44 pm]

Too busy to listen to NPR, even. So I missed what apparently was a great bit by [Andrei Condrescu](#) (who has a great radio voice and a truly tilted look at things) finding some interesting parallels to blogs in nature – Read [Doc Searl's writeup](#) or listen to it yourself: [Working For Nothing?](#)

[permalink to just this entry](#)

[Steven Levy on Trusted Computing in Newsweek](#) [9:48 am]

[A Net of Control](#) [via [BoingBoing](#)] [[pdf](#)]

Picture, if you will, an information infrastructure that encourages censorship, surveillance and suppression of the creative impulse. Where anonymity is outlawed and every penny spent is accounted for. Where the powers that be can smother subversive (or economically competitive) ideas in the cradle, and no one can publish even a laundry list without the imprimatur of Big Brother. Some prognosticators are saying that such a construct is nearly inevitable. And this infrastructure is none other than the former paradise of rebels and free-speechers: the Internet.

Donna's comments at [Copyfight](#)

[permalink to just this entry](#)

[A Compulsory Licensing Discussion](#) [8:42 am]

Start here with Donna tracking the start: [Compulsory Licensing: Where's the Beef?](#)

I have to admit that I fall into the Felten camp on this one; monitoring network traffic to manage P2P exchanges just reeks of geometric complexity, particularly in the face of a desire to circumvent/manipulate the system. I don't yet see the necessary holy grail – a system that monitors without engendering large enough economic incentives to circumvent and/or manipulate that it will be worth doing. Given the copyright industry mindset, I cannot imagine them electing to choose an imperfect system of weak copyright in this space – rather, they're going to want a centralized, fully dominating approach, thereby engendering the incentives to circumvent.

The compromises with liberty crafted to promote creativity through monopoly look terribly bad when it actually becomes possible to enforce that monopoly thoroughly and pervasively. And, as far as I can see to this point, the technical approaches cited as necessary tools



for compulsory licensing can also be used to achieve more repressive compensation schemes – not a set of toys to give to the RIAAs of the world!

Maybe I'm missing something – I hope so, because the buzz around compulsory licensing keeps getting louder.....

[permalink to just this entry](#)

## [Morning Chuckle](#) [7:54 am]

From yesterday's *Register*: [RIAA hires guns, alcohol and smokes expert to fight piracy](#)

“It's hard to convince fans to pay up when everyone knows artists get only pennies from a \$16 CD,” said Downhill Battle. “Since major labels can't convince people, they need to coerce them. But if the RIAA has the same success stopping downloading as the ATF has had stopping illegal gun sales, then we don't think filesharers have a lot to worry about. Parallels to the prohibition are rife: free, non-DRM music is just too popular. [Former ATF chief] Bradley A. Buckles will be playing a losing game of gangbusters.”

Donna's comments: [Alcohol, Tobacco, Firearms, Explosives](#)

[permalink to just this entry](#)

## Tuesday, December 9

### [eWeek Editorial](#) [6:46 pm]

[Copyright and Fair Use](#): *Repeated abuse of a statute is a sign that the law itself is defective.*

The Skylink and Lexmark examples show that the DMCA is disturbingly susceptible to use as an anti-competitive weapon. Repeated abuse of a statute in this way is a sign that the law itself is defective. We call upon legislators and the courts to attain a balance that will promote the interests of copyright owners while respecting the rights of consumers. Thus, we back U.S. Rep. Rick Boucher's H.R. 107, under which circumvention for the purpose of exercising fair-use rights would be allowed. The Virginia Democrat's bill would also allow making and distributing hardware and software if the technology is capable of substantial noninfringing use.

[permalink to just this entry](#)

### [A Re-Examination of the FAT Patents?](#) [6:28 pm]

Probably not what Microsoft had in mind when they offered to license some of their technology – but is this just wishful thinking on Andrew Orłowski's part?: [Microsoft FAT patents 'could be re-opened'](#)

If Microsoft decides to mine its patent portfolio for cash, it's likely to face a few unexpected consequences. A new patent body that's vowing to defend the free software community against Microsoft's new patents-for-cash revenue strategy says it will ask the US Patent Office to go back to square one, and systematically examine the validity of the patents in question. This is an unusual tactic that promises to bring the overworked USPTO's approval of questionable patents right into the spotlight.

[...] The [Public Patent Foundation](#)'s mission is to advise and counsel people who object to patents that threaten to “restrict civil liberties and free markets”, Dan tells us. The PPF has other options including filing friend of the court briefs on behalf of defendants, and broader education. He's keen to encourage companies form mutually beneficial “disarmament treaties”, too.

[permalink to just this entry](#)

### [Jobs on Music](#) [6:21 pm]

Steven Jobs is interviewed in Rolling Stone: [Steve Jobs: The Rolling Stone Interview](#): *He changed the computer industry. Now he's after the music business.* (Slashdot discussion: [Steve Jobs and the State of Legal Music Downloads](#))

Interesting to see just how hard it is for him to make his case:

**David Bowie predicted that, because of the Internet and piracy, copyright is going to be dead in ten years. Do you agree?**

No. If copyright dies, if patents die, if the protection of intellectual property is eroded, then people will stop investing. That hurts everyone. People need to have the incentive so that if they invest and succeed, they can make a fair profit. But on another level entirely, it's just wrong to steal. Or let's put it this way: It is corrosive to one's character to steal. We want to provide a legal alternative.

**Of course, a lot of college students who are grabbing music off Kazaa today don't see themselves as doing anything any different from what you did when you were a teenager, copying bootleg Bob Dylan tapes.**

The truth is, it's really hard to talk to people about not stealing music when there's no legal alternative. The advent of a legal alternative is only six months old. Maybe there's been a generation of kids lost – and maybe not, who knows? Maybe they think stealing music is like driving seventy mph on the freeway – it's over the speed limit, but what's the big deal? But I don't think that's the way it's going to stay, not with future generations, at least. But who knows? This is all new territory.

There's a contradiction at the heart of what he's trying to say. For example, there's this:

**Of course, music theft is nothing new. There have been bootlegs for years.**

Of course. What's new is this amazingly efficient distribution system for stolen property, called the Internet – and no one's gonna shut down the Internet.

And it only takes one stolen copy to be on the Internet. The way we expressed it to them was: You only have to pick one lock to open every door.

And yet, he gets what really needs to be sold to compete with “free:”

Our position from the beginning has been that eighty percent of the people stealing music online don't really want to be thieves. But that is such a compelling way to get music. It's instant gratification. You don't have to go to the record store; the music's already digitized, so you don't have to rip the CD. It's so compelling that people are willing to become thieves to do it. But to tell them that they should stop being thieves – without a legal alternative that offers those same benefits – rings hollow. We said, “We don't see how you convince people to stop being thieves unless you can offer them a carrot – not just a stick.” And the carrot is: We're gonna offer you a better experience . . . and it's only gonna cost you a dollar a song.

The other thing we told the record companies was that if you go to Kazaa to download a song, the experience is not very good. You type in a song name, you don't get back a song – you get a hundred, on a hundred different computers. You try to download one, and, you know, the person has a slow connection, and it craps out. And after two or three have crapped out, you finally download a song, and four seconds are cut off, because it was encoded by a ten-year-old. By the time you get your song, it's taken fifteen minutes. So that means you can download four an hour. Now some people are willing to do that. But a lot of people aren't.

Not to mention explaining the record industry/artist conflict succinctly:

**They feel they've been ripped off.**

They feel that. But then again, the music companies aren't making a lot of money right now . . . so where's the money going? Is it inefficiency? Is somebody going to Argentina with suitcases full of hundred-dollar bills? What's going on?

After talking to a lot of people, this is my conclusion: A young artist gets signed, and he or she gets a big advance – a million dollars, or more. And the theory is that the record company will earn back that advance when the artist is successful.

Except that even though they're really good at picking, only one or two out of the ten that they pick is successful. And so

most of the artists never earn back that advance – so the record companies are out that money. Well, who pays for the ones that are the losers?

The winners pay. The winners pay for the losers, and the winners are not seeing rewards commensurate with their success. And they get upset. So what's the remedy? The remedy is to stop paying advances. The remedy is to go to a gross-revenues deal and tell an artist, "We'll give you twenty cents on every dollar we get, but we're not gonna give you an advance. The accounting will be simple: We're gonna pay you not on profits – we're gonna pay you off revenues. It's very simple: The more successful you are, the more you'll earn. But if you're not successful, you will not earn a dime. We'll go ahead and risk some marketing money on you. But if you're not successful, you'll make no money. If you are, you'll make a lot more money." That's the way out. That's the way the rest of the world works.

**So you see the recording industry moving in that direction?**

No. I said I think that's the remedy. Whether the patient will swallow the medicine is another question.

[permalink to just this entry](#)

## [Media Consolidation – VoIP Meets Cable](#) [6:02 pm]

NYTimes: [Time Warner to Use Cable Lines to Add Phone to Internet Service](#); CNet News: [Time Warner Cable reaches VoIP deals](#)

I *know* I read something about the competitiveness issues around this move, but I can't find it. Consider, though, what the opportunities are for bundling. With luck, I'll find it eventually.

[permalink to just this entry](#)

## [Derek's First Report On the ACS Meeting](#) [11:59 am]

### [ACS Meeting Report, Pt 1](#)

I came out of the meeting a lot more interested in what comes in-between where we are now and a mandatory compulsory licensing model - that is, something like Professor Fisher's voluntary co-op idea. Right now, there is little chance the record industry will voluntarily offer blanket licenses. Digital music services will continue to evolve, but it will be a long time before they attempt to realize the potential of the Internet and create a model that does not depend on controlling all copying and distribution. So someone outside the current industry would have to step up to demonstrate the model's potential. The value in that demonstration, whether it leads to a government-mandated or market model, is significant.

[...] One key thread that came up during both this conference and the Gartner/Berkman conference is that norms will factor in to a large extent. The voluntary co-op model would comport with people's norms, in that it would not allow people to download and upload content on P2P, as long as it was authorized by that voluntary ACS. However, that is not a guarantee that it can compete with free.

[permalink to just this entry](#)

## [Benny Evangelista on the Music Conference](#) [11:53 am]

### [Online music on center stage: Conference grapples with new digital world](#)

Some interesting quotes:

"Since the first century, music has always had the same business," said Ron Stone, founder of artist management agency Gold Mountain Entertainment. "We play music, you like it, you pay us money." Later, he noted how file sharing has devalued music. "Music for a generation has become disposable and it used to be a collectible," Stone said.

Other new research showed the future of the record industry might harken to its past, when 45 rpm singles ruled the charts. The NPD Group found consumers who used licensed online music services downloaded just one or two songs from an album 94 percent of the time. Consumers downloaded five or more songs only 2 percent of the time, NPD said.

Most the songs downloaded were older songs from an artist's catalog: 18 percent of the songs were released after February 2002 and 82 percent were songs older than that.

"It makes sense to offer a discount when consumers buy four or five songs from the same artist, regardless of what album they originate from," Crupnick said. "Less-popular tracks offered as free downloads might even be effectively leveraged to market paid downloads of more popular songs and drive sales of full CDs."

However, the study didn't jibe with Apple Computer's data that 45 percent of the songs downloaded using iTunes Music Store were whole albums.

"Collectible" – somehow, I think of the Franklin Mint when I hear that word, not the music that I have and enjoy. And, when it comes to collectible, I'm surprised to see a claim that digital downloads have limited collections. My experience with music downloaders is that they have stored more music on their hard disks than they can ever expect to listen to – in fact, the size of their collection is a key factor in their continuing efforts to expand it.

[permalink to just this entry](#)

## [More on Music Pricing](#) [10:51 am]

CNet News: [How much is digital music worth?](#)

Speaking at the iHollywood Forum's Music 2.0 conference in Los Angeles Monday, executives on both sides focused on the 99-cent price tag that has become the market's standard for downloadable music.

Critics say that that price needs to come down if mainstream consumers are to start buying in large numbers, making the Internet a serious factor in the record industry's bottom line. Record labels say they can't afford to go lower.

"There's very little money in this to begin with," said David Ring, vice president of Universal Music Group's eLabs division. "A lot of people are already recognizing that we're going to have to sell a lot more singles at 99 cents in order for us to make money, and for artists to be able to make a living."

[...] Despite these positive early signs from iTunes and its rival services, consumers are still showing resistance to today's prevailing market price for digital music, conference attendees said.

"I've been hearing 99 cents (as a price for digital songs). If it's that, I would just go out and buy the CD," said Alina, a UCLA student who participated on a panel discussing college students' music behavior.

She said she had never used any of the paid digital music services. The students did not use their full names, in part because in some cases they were talking about downloading music illegally. "If it's 30 cents I would buy it."

[...] "There has not really been an attempt to explore the price elasticity of this product," said Robbie Vann-Adibe, CEO of Ecast, a company that provides digital music jukeboxes for bars and retail businesses.

Currently, close to two-thirds of the 99 cent digital song price goes to labels and other copyright holders, leaving slim or even negative margins for the song stores themselves. Apple CEO Steve Jobs recently said his company remains interested in the business because it helps sell the company's profitable iPod music devices.

[permalink to just this entry](#)

## [Things Go Better With Coke](#) [8:16 am]

The next wave of corporate sponsorship for music continues – [Coke floats music download service](#)

In January of next year, the myCoke Music site will go live in the U.K. Coke has promised a selection of over 250,000 songs from 8,500 artists at a cost of 99p each. The new service will be run in partnership with music distributor OD2 - Microsoft's European DRM supplier.

You've got to admire the tremendous sack of a company that can pull off handing kiddies teeth-rotting drinks with one

hand while serving up a DRM infection with the other. The cunning marketeers at Coke, however, are one step behind rival Pepsi, which already announced a deal with Apple to give 100 million iTunes songs. But Apple has yet to roll out a Euro service, and Coke is stepping up to give the UK kiddies what they want.

In different shapes and forms, we now have Apple, Microsoft, Dell, HP, Napster, Pepsi, Coke and maybe even Wal-Mart hawking songs online. All of these companies are rushing to enter a business with atom thin margins at best and business sinking losses at worst. In almost every case, the motive is to link to a larger sale be it pricey iPods or placing a brand in the consumer's face for other, profit-making goods.

Update: CNet News with the Reuters feed: [Call it pop—Coke to launch online music service](#)

[permalink to just this entry](#)

## Monday, December 8

### [Doc Pulls Together...](#) [3:51 pm]

Pieces that nail what I didn't like about the NYTimes Magazine [article on the Dean campaign](#). See it all in his posting, [Same Times](#)

[permalink to just this entry](#)

### [Lessig on Latter-Day Winston Smiths](#) [3:27 pm]

And finding their handiwork with the [Wayback Machine](#): [speaking of new speak, a report from the Archives](#)

On May 1, 2003, the Whitehouse's Office of the Press Secretary released [this](#) press release, announcing "President Bush Announces Combat Operations in Iraq Have Ended." But then, with airbrush magic, now the same press release has been changed to [this](#), which reports "President Bush Announces Major Combat Operations in Iraq Have Ended." No update on the page, no indication of when the change occurred, indeed, no indication that any change occurred at all. Instead, there is [robots.txt](#) file disallowing all sorts of activities that might verify the government. (Why does any government agency believe it has the power to post a robots.txt file?)

Why would you need to check up on the Whitehouse, you might ask? Who would be so unAmerican as to doubt the veracity of the Press Office? Great question for these queered times. And if you obey the code of the robots.txt file, you'll never need to worry.

[permalink to just this entry](#)

### [WSIS Info](#) [2:56 pm]

In re the WSIS matters that are [cropping up all over](#), here's the WWW page for the [WSIS Civil Working Group: Patents, Copyrights and Trademarks](#), which has an [action plan](#) for the upcoming meeting. Note that Richard Stallman is on the [Steering Committee](#) for this group; and Larry Lessig is on the [Agenda](#) for a Friday Roundtable.

(Slashdot discussion: [World Summit On The Internet And IT](#))

Note that there will be some interesting opportunities to kick in your opinion: [Go Tell It on the Mountain](#)

Diplomats from 191 countries meet this week in Geneva for the three-day United Nations World Summit on the Information Society. It's the occasion for [The Helloworld Project](#) to project thousands of 500-foot-high laser-light SMS messages onto the Geneva fountain.

Internet users everywhere can post billboard thoughts almost instantly onto the fountain – or onto the northern façade of New York's U.N. building, the face of a mountain in Rio de Janeiro or the front of a Bombay skyscraper.

"The idea is to use the media to allow people to get their message across to powerful people," said Swiss Web designer Johannes Gees, who conceived, coordinated and sought funding for the \$250,000 Helloworld Project. The project is similar

to a smaller version he implemented at the 2001 World Economic Forum.

Anyone can use a website form or send an SMS to create a message and project it across any or all of the four global landmarks with 10- to 20-watt semiconductor lasers. Of course, Internet access hasn't yet reached all corners of the world – that's why the United Nations is having the meeting.

[permalink to just this entry](#)

## [Pew's Query of the Moment](#) [2:35 pm]

Pew's [Internet and American Life Project](#) has posted a quite interesting "Query of the Moment" on their front page:

Are you an artist – musician, writer, painter, or other type of artist? We would like to know how you use the Internet and your views on copyright issues. Specifically, what's your opinion about file-sharing programs and their impact on the artistic community?

Click here to answer (go there to do so for real)

I look forward to hearing what comes of this one...

[permalink to just this entry](#)

## [CD Pricing Study](#) [2:29 pm]

From Ipsos-Insight's [TEMPO](#) (cited last week in some circles) : [Consumers Expect Substantial Savings On Digitally Distributed Albums](#)

Regardless of downloading experience, American Internet users aged 12 and older stated an acceptable price range of \$9.99 to \$14.99 for a new, full-length physical CD release. In contrast, the acceptable price range for a digitally distributed, full-length album download is only between \$5.00 and \$9.99 – roughly \$5.00 less than for a physical CD. These findings are based on recent interviews conducted with a representative U.S. sample of 488 Internet users aged 12 and over.

“A roughly \$5.00 decrease in the range of acceptable prices for a new, full length album distributed digitally versus in a physical format represents a significant decrease in perceived value for this product based solely on format or distribution method,” stated Matt Kleinschmit, a director of research at [Ipsos-Insight](#), and the study's author.

The research also found that these price expectations for a physical CD were consistent regardless of downloading experience, suggesting that lower prices for digitally distributed music are expected even among consumers who have not downloaded music.

“This may be indicative of a broader re-examination of the perceived value of music by consumers, in that they may be willing to pay more for a durable product that is perceived as more permanent and archival in nature, rather than a digital format that may be viewed as more temporary.”

[...] “Two important points emerged from our study. First, the price points that will maximize consumer adoption for both physical CDs and album downloads are much lower than those currently found in the marketplace. This suggests that recently launched online music services and traditional music retailers, both of whom are actively struggling to lure buyers to boost lagging music sales, may benefit from a more conservative pricing strategy. Second, the relative lack in purchase intent for a digitally distributed, full-length album download even at a \$7.99 price-point is also surprising, and may indicate that consumers view digital distribution as a purchase channel primarily for individual songs or tracks, and prefer to purchase a physical CDs when they want to own the entire album.”

[permalink to just this entry](#)

## [Umberto Eco on "Vegetal Memory"](#) [9:32 am]

From kuro5hin: [In Defense of Vegetal Memory](#) - on Eco's lecture [Vegetal and mineral memory: The future of books](#) (too bad he didn't touch on access as an issue)

We have three types of memory. The first one is organic, which is the memory made of flesh and blood and the one administrated by our brain. The second is mineral, and in this sense mankind has known two kinds of mineral memory: millennia ago, this was the memory represented by clay tablets and obelisks, pretty well known in this country, on which people carved their texts. However, this second type is also the electronic memory of today's computers, based upon silicon. We have also known another kind of memory, the vegetal one, the one represented by the first papyruses, again well known in this country, and then on books, made of paper. Let me disregard the fact that at a certain moment the vellum of the first codices were of an organic origin, and the fact that the first paper was made with rugs and not with wood. Let me speak for the sake of simplicity of vegetal memory in order to designate books.

[...] After having spent 12 hours at a computer console, my eyes are like two tennis balls, and I feel the need of sitting down comfortably in an armchair and reading a newspaper, or maybe a good poem. Therefore, I think that computers are diffusing a new form of literacy, but they are incapable of satisfying all the intellectual needs they are stimulating. Please remember that both the Hebrew and the early Arab civilisations were based upon a book and this is not independent of the fact that they were both nomadic civilisations. The Ancient Egyptians could carve their records on stone obelisks: Moses and Muhammad could not. If you want to cross the Red Sea, or to go from the Arabian peninsula to Spain, a scroll is a more practical instrument for recording and transporting the Bible or the Koran than is an obelisk. This is why these two civilisations based upon a book privileged writing over images. But books also have another advantage in respect to computers. Even if printed on modern acid paper, which lasts only 70 years or so, they are more durable than magnetic supports. Moreover, they do not suffer from power shortages and black-outs, and they are more resistant to shocks.

Up to now, books still represent the most economical, flexible, wash-and-wear way to transport information at a very low cost. Computer communication travels ahead of you; books travel with you and at your speed. If you are shipwrecked on a desert island, where you don't have the option of plugging in a computer, a book is still a valuable instrument. Even if your computer has solar batteries, you cannot easily read it while lying in a hammock. Books are still the best companions for a shipwreck, or for the day after the night before. Books belong to those kinds of instruments that, once invented, have not been further improved because they are already alright, such as the hammer, the knife, spoon or scissors.

[...] Alas, with an already written book, whose fate is determined by repressive, authorial decision, we cannot do this. We are obliged to accept fate and to realise that we are unable to change destiny. A hypertextual and interactive novel allows us to practice freedom and creativity, and I hope that such inventive activity will be implemented in the schools of the future. But the already and definitely written novel War and Peace does not confront us with the unlimited possibilities of our imagination, but with the severe laws governing life and death.

[...] Indeed, in a role-play game one could rewrite Waterloo such that Grouchy arrived with his men to rescue Napoleon. But the tragic beauty of Hugo's Waterloo is that the readers feel that things happen independently of their wishes. The charm of tragic literature is that we feel that its heroes could have escaped their fate but they do not succeed because of their weakness, their pride, or their blindness. Besides, Hugo tells us, "Such a vertigo, such an error, such a ruin, such a fall that astonished the whole of history, is it something without a cause? No... the disappearance of that great man was necessary for the coming of the new century. Someone, to whom none can object, took care of the event... God passed over there, *Dieu a passé.*"

That is what every great book tells us, that God passed there, and He passed for the believer as well as for the sceptic. There are books that we cannot re-write because their function is to teach us about necessity, and only if they are respected such as they are can they provide us with such wisdom. Their repressive lesson is indispensable for reaching a higher state of intellectual and moral freedom.

[permalink to just this entry](#)

## [Nice SCO Spoof](#) [8:45 am]

Incorporating recent news: [SCO Must Prove Existence Of Santa Claus in Thirty Days](#)

Supreme Court Judge Isaiah Moore ruled that SCO must show proof of Santa Claus in the next 30 days, or he will dismiss their lawsuit against all Christians and companies profiting from the Christmas holiday.

SCO, formerly known as Santa Cruz Operations, recently changed their name to Santa Claus Operations. This change was widely regarded as a move to improve their image after their controversial claims about Linux. Critics of the name change say it's just another fantasy created by SCO CEO Kris Kringle, formerly known as Darl McBride, to profit through litigation.

In a recent press release SCO said it would begin sending out invoices to anyone who celebrates or profits from Christmas in the next couple of weeks including corporations and individuals. A price list for SCO Christmas licenses which companies and individuals need to celebrate the holiday without violating SCO's intellectual property rights were released as well.

[permalink to just this entry](#)

## [International Technology Policy](#) [8:18 am]

### [Nations Chafe at U.S. Influence Over the Internet](#)

Icann and the United States government are expected to come under heavy fire at the conference, which begins Wednesday in Geneva and will be one of the largest gatherings of high-level government officials, business leaders and nonprofit organizations to discuss the Internet's future. An important point of debate will be whether the Internet should be overseen by the United Nations instead of American groups like Icann.

"I am not amused," Mr. Twomey said via a cellphone outside the conference room Friday evening after he was barred from the planning meeting. "At Icann, anybody can attend meetings, appeal decisions or go to ombudsmen. And here I am outside a U.N. meeting room where diplomats - most of whom know little about the technical aspects - are deciding in a closed forum how 750 million people should reach the Internet." Mr. Twomey said that others were also kept out, including members of the news media and anyone who was not a government official.

[...] Because the Internet first took root in the United States, it may be understandable that American interests have tended to prevail. The Massachusetts Institute of Technology, for example, still has more Internet addresses than all of China, according to Lee McKnight, an associate professor at Syracuse University and an M.I.T. research affiliate.

The joys of owning a Class A IP address..... And here's some clever rhetorical ju-jitsu, equating the technical performance of the Internet with the policy/oversight performance of ICANN:

But, he said, when it comes to the technical underpinnings of the Internet, Icann should be allowed to continue its work, Mr. Twomey said. "It is not broken, so why fix it?"

See also [Internet showdown side-stepped in Geneva](#); also a Slashdot discussion: [World Summit On The Internet And IT](#)

[permalink to just this entry](#)

## [Trojan P2P Nets](#) [8:13 am]

The NYTimes discusses the rise of the Trojan-based P2P network in [Hackers Steal From Pirates, to No Good End \(CNet's version\)](#). What's particularly notable, assuming that it's legit, is the series of discussions cited with an online seller of spam services via a Trojan P2P net:

"Sinit appears to have been created as a money-making endeavor," Mr. Stewart said in a research paper describing his discovery. "This Trojan is also further evidence that money, not notoriety, is now the major driving force behind the spread of malware these days."

There is now a market for the services of networks of infected machines, which can allow illicit operators to carry out scams and activities prohibited by legitimate Internet service providers. On Web sites frequented by hackers, spammers and people who identify themselves as practitioners of credit card fraud, the remote-access networks, or "radmins," are offered openly.

On one such site, Carder Planet, a typical pitch from "r00t3d" reads, "I have a steady supply of FAST radmins. I am wanting to offer these to those of you who need good hosting for your scam pages" for periods of a week to "six months or more" for a price of \$50 per machine.

The hacker did not respond to online requests for further information, but in a general discussion on the site he defended his work on Trojan-infected machines by saying "money makes this forum and the world go around." He added that "spam page hosting is obviously needed," and therefore, "people will purchase that service."



The implications for the Internet of the new breed of Trojan programs are troubling, said Bruce Schneier, the founder and chief technical officer of Counterpane Internet Security Inc. “A self-replicating peer-to-peer network is kind of scary,” he said, not just because a less easily detectable network is bad news, but because it offers proof that hackers, once primarily interested in breaking into systems for thrills, now have a profit motive.

[permalink to just this entry](#)

## [Innovation – Just What This Market Needs](#) [8:06 am]

### [A New Use for a CD's Flip Side](#)

OneDisc Technologies of Dallas is in talks with major and independent labels to begin making a combination single-disc product that plays DVD video on one side and CD audio on the other, the company's president, James Wilson, said.

A combination disc from the singer-songwriter Kathleen Edwards, “Live From the Bowery Ballroom” on Rounder Records, is already in stores. One side includes three songs that play in a standard CD player, while the flip side features two DVD music videos. OneDisc owns a license for the technology involved.

For years, artists have included video footage on enhanced music CD's, but that video, viewable on a computer as a CD-ROM, does not have the same playback quality of DVD's. More recently, record labels have been bundling bonus DVD's with traditional CD's to entice music fans to buy albums rather than illegally downloading or copying them. Those packages include two separate discs, one for audio content and other for video.

“The problem here, in general for the music industry, is that the value of the piece of plastic that has the music on it is going down,” Josh Bernoff, a principal analyst with Forrester Research, said.

The Forrester quote is pretty stupid, really – the piece of plastic has never been valuable. But the real point is legitimate; digital distribution means that the CD as a delivery vehicle has to compete on new fronts, and it has done so imperfectly. After all, the bandwidth in CD delivery is pretty substantial – it's just that, more and more, the whole album is not what the consumer demands.

[permalink to just this entry](#)

## [Google-washing Redux](#) [7:57 am]

### [Foes of Bush Enlist Google to Make Point](#)

Anyone searching on Google for the phrase “miserable failure” was sent to the official White House biography of President Bush.

Google executives say they have no corporate opinion of the Bush presidency. Instead, the episode is another example of a form of cyber-graffiti known as “Google bombing.”

It is a group prank. If enough Web pages link a certain Web page to a phrase, the Google search engine will start to associate that page with the phrase - even if, as in the case of Mr. Bush's official biography, the phrase does not occur on the destination Web site

I post this only to demonstrate just how poorly educated some corporate IS firms are. My wife's been trying to learn from her IS group about Google rankings, and their responses to her have been tragically uninformed – an Amazonian headhunter could come up with a better explanation than some of the nonsense she's shown me in their e-mails. Yet, here are some hackers readily manipulating the system.

On the other hand, it's also clear that Google doesn't quite get it either, as this quote reveals:

Craig Silverstein, Google's director for technology, says the company sees nothing wrong with the public using its search engine this way. No user is hurt, he said, because there is no clearly legitimate site for “miserable failure” being pushed aside.

I'd love to know what Mr. Silverstein's definition of "legitimate" is.

[permalink to just this entry](#)

## [Oops](#) [7:54 am]

Mary Hodder points out that yesterday's "Catching Up" posting exposes not so much how far behind I am, as it demonstrates the limitations of my RSS aggregator. October NYTimes articles, indeed. In fact, I'm pretty sure I cited them already. Must have been \*really\* worn out from shoveling.

While RSS aggregators have been somewhat useful to me when I'm in a hurry, I'm less enamored of them when I have a little more time. But, maybe that's just the limitations/problems with the one I'm working with these days. Anyway, my apologies.

[permalink to just this entry](#)

## Sunday, December 7

### [Catching up.....](#) [4:56 pm]

- CNet: [Hollywood: Norwegian hacker a burglar](#)

"We consider this stealing," Marsha King, executive vice president and general manager of Warner Home Video, told the Oslo Appeals Court. "It's taking our key and breaking into our house and stealing what we've made," she said.

Good luck finding a judge dumb enough to buy that argument

- CNet: Some compulsory licensing thoughts, inspired by the Canadian record industry's initiative – [Should ISP subscribers pay for P2P?](#)
- NYTimes' David Pogue: [The File-Sharing Debates](#)

Last week in this space, I wondered why the RIAA (Recording Industry Association of America) and movie studios get so worked up about online file swapping, when public libraries distribute their works freely without a penny of compensation.

As usual, some of this column's readers responded thoughtfully and with authority; I thought I'd share three of those reactions with you this week.

- NYTimes: [Online Music Business, Neither Quick Nor Sure](#) – surprise.....

[permalink to just this entry](#)

### [A look at our snow](#) [12:04 pm]

The image with the yellowish cast is from last night at about 10:00 PM. I got up this morning to what looks to have been another 6 inches (although it could have just been drifts – the wind was really howling). They're saying Boston got about 16 inches. This \*so\* not typical for December. (Gov. Menino is on the TV telling us that Boston schools will be closed tomorrow). Let's just say that the weekend has been devoted to shoveling and not a lot of web browsing or generally catching up.....



Update: Here are a couple from the front of my home, following a morning of shoveling, and one looking out the back onto the deck – note that it's still coming down, but not quite so hard anymore.....

[permalink to just this entry](#)

### [KaZaA Lite Shutdown by Sharman](#) [11:45 am]

According to Slashdot, via [Zeropaaid](#), KaZaA Lite has been shutdown: [Kazaa-lite Shut Down](#)

Interesting – with Zeropaaid Slashdotted, I thought I'd see what I could do to try to find other ways in using a Google [search for Kazaa-lite](#) and I got an interesting notice: "In response to a complaint we received under the [Digital Millennium Copyright Act](#), we have removed 3 result(s) from this page. If you wish, you may [read the DMCA complaint](#) for these removed results." – a cute way around the requirement, since of course the complaint has to be public.

The subtler question is the question of whether Google has cross referenced all 11 complaints filed at Chilling Effects against the sites that come up in a Google search. See [Chilling Effect's search page](#) (search for keywords "kazaa" and "google") to see all 11 complaints.

[permalink to just this entry](#)

## Saturday, December 6

### [Ed Felten on the Alternative Compensation Meeting](#) [11:34 pm]

Ed has posted his thoughts on the Alternative Compensation Meeting here: [Reflections on the Harvard Alternative Compensation Meeting](#). He mentions that the weather has kept him in the city for a while (Logan's been closed most of the day.) Sorry I didn't get a chance to meet him.....

The afternoon discussion was about voluntary license schemes. And here an interesting thing happened. We talked for a while about how one might structure a system in which consumers can license a pool of copyrighted music contributed by artists, with the revenue being split up appropriately among the artists. Eventually it became clear that what we were really doing was setting up a record company! We were talking about how to recruit artists, what contract to sign with artists, which distribution channels to use, how to price the product, and what to do about P2P piracy of our works. Give us shiny suits, stubble, tiny earpiece phones, and obsequious personal assistants, and we could join the RIAA. This kind of voluntary scheme is not an alternative to the existing system, but just another entrant into it.

Mary Hodder's [tracking other postings](#) on the subject.

[permalink to just this entry](#)

### [Zack in the NYTimes Magazine](#) [1:50 pm]

Nothing like a snowstorm to give you the time to work through the Saturday and the part of the Sunday NYTimes. So, I got to see that [Zack Rosen](#) (from [ILaw 2003](#) at Stanford) gets some ink and a photo in the Magazine section. An odd slant on what brings people to Dean, but a good look at Zack (left in the photo to the right). Check it out: [The Dean Connection \[pdf\]](#)



Zack Rosen was a creator of DeanSpace, “the revolution itself.” He started the project, originally called Hack for Dean, after reading about Dean on the campaign Web site for 20 minutes. “I just knew this is the guy,” Rosen says. He recruited an unpaid team of nearly a hundred programmers, including his friends Neil and Ping, to write software for the campaign that would allow the many disparate, unofficial Dean Web sites to communicate directly with one another and also with the campaign. Typically, to reproduce information from one Web site to another, a user has to cut the information by hand and paste it into each Web site, a laborious process. The software that Zack’s group built allows any Dean Web site to reprint another’s stories, images and campaign feed automatically, as if they have a collective consciousness. It also will provide a “dashboard” for the people in Burlington, where the campaign can track patterns on its unofficial sites and observe which content is most popular.

[...] It’s not hard to imagine that if the year were 1999, Rosen, an ambitious college kid with an exciting new software idea, could be easily recast in the role of child tycoon. But Rosen isn’t mourning being born a few years too late. It is not clear to him who owns the programs he invented – the Democratic National Committee? Howard Dean? – but he doesn’t really care.

Rosen says the true purpose of the Internet is to allow people to connect, and he isn’t surprised there wasn’t money to be made on that premise. Through his long fluorescent nights, Rosen takes breaks from coding to gaze happily at the personal e-mail messages Dean supporters compose and send using Dean software. “Look,” he says wistfully, the light of the computer reflecting off of his glasses. “This is Nelson. He spent real time on this letter. Look how long it is.”

Rosen is one of the more diehard programmers at the Dean office. He can easily discourse for half an hour about “open-source political campaigns” or the possibility of using cellphones to overthrow dictatorships or “recursive hard core CS225 data structures.” But he surprises me by saying he never would have come up with the Dean software, or left school, if his first serious girlfriend (like Johnson’s crush also named, coincidentally, Julie) hadn’t broken up with him last spring.

“The worst thing is we aren’t even friends,” he says glumly. “I invited her to be my friend” – he gestures to his computer monitor – “I mean on Friendster. No word yet.”

[...] Watching [Zack and his crew] work from their battered easy chair, I find it impossible to tell if they are gazing at the filmy, pixilated image of a Julie or the face of a new Dean supporter or a line of code; whether the peer-to-peer communication they are struggling with is related to the 2004 election and the fragmentation of American public life, or is something more private.

While the Times article seems to be arguing that people come to Dean to fill a missing piece of their lives, I’m not exactly sure why that’s supposed to be news. The very fact that they form a community is a strength, not terribly different from a host of other human activities. And the fact that the network has been an instrument in building that community has proven to be very powerful.

Update: Note that [Doc Searls](#) has assembled a number of comments that explain the issue I have with this writeup better than I did.

[permalink to just this entry](#)

## Friday, December 5

### [SCO Has To Go First](#) [6:13 pm]

[Slashdot](#) is full of the [GrokLaw reports](#) that SCO lost both motions today in Utah, and has 30 days to produce *all* the supposedly infringing code.

Cool, but I like the fact that GrokLaw notes elsewhere that Linus Torvalds is getting his hands dirty after asserting that the law was to be left to lawyers. See [Linus Digs Into Copyright Law and Notices Something Useful](#) – a response to [Slashdot on Daryl McBride’s Latest \(updated\)](#)

I ended up looking up the exact wording of the US copyright law for the definition of ‘derivative’, and guess what I find a few lines below it:

The term “financial gain” includes receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works.

This is from US Code Collection, Title 17 (copyrights), Chapter 1, Section 101: ‘Definitions’. In short, this is from the very first section in copyright law - the thing that defines terms even before those terms are used. What I’m trying to say - this is some pretty fundamental stuff when it comes to copyrights in the US. Pertinent, if you will.

And note how copyright law expressly includes ‘the expectation of receipt’ of anything of value, and expressly mentions ‘receipt of other copyrighted works’ as such a thing of value. And that’s the definition of ‘financial gain’ as far as copyright law is concerned.

And guess what the GPL is all about? Maybe you can explain to Darl how the GPL is designed so that people receive the value of other peoples copyrighted works in return for having made their own contributions. That is the fundamental idea of the whole license - everything else is just legal fluff.

[permalink to just this entry](#)

### [Slashdot on Daryl McBride’s Latest \(updated\)](#) [9:34 am]

True, it’s clearly flamebait, and Slashdot rises to it: [McBride’s New Open Letter on Copyrights](#). The [letter/press release](#) is a look into a seriously peculiar interpretation of the GPL, but what would you expect?

However, there is a group of software developers in the United States, and other parts of the world, that do not believe in the approach to copyright protection mandated by Congress. In the past 20 years, the Free Software Foundation and others in the Open Source software movement have set out to actively and intentionally undermine the U.S. and European systems of copyrights and patents. Leaders of the FSF have spent great efforts, written numerous articles and sometimes enforced the provisions of the GPL as part of a deeply held belief in the need to undermine or eliminate software patent and copyright laws.

The software license adopted by the GPL is called “copy left ” by its authors. This is because the GPL has the effect of requiring free and open access to Linux (and other) software code and prohibits any proprietary use thereof. As a result, the GPL is exactly opposite in its effect from the “copy right ” laws adopted by the US Congress and the European Union.

Uh-huh. Except, of course, that the GPL’s legal force derives from the very copyright laws that Mr. McBride asserts that it acts to subvert. Apparently, there are only some things one is allowed to do with one’s monopoly, and electing to use it to do something other than to extract monopoly rents is unconstitutional. I wonder if all of Mr. McBride’s life is governed by marketplace behavior – life at home must be pretty interesting.

And dragging *Eldred v. Ashcroft* into the discussion is just tragic.

Update: As usual, for the straight poop, see [GrokLaw](#), particularly the **excellent** [Darl’s “Greed is Good” Manifesto](#) – an excellent reminder that liberty, not profit, underlies the American experiment in government. Note that, according to GrokLaw, the site is [cited in IBM’s recent reply briefs](#) in advance of today’s hearings in Utah. The power of community.....

[permalink to just this entry](#)

### [All Your FAT Are Belong To Us \(sorry\)](#) [7:22 am]

- Slashdot – [Microsoft to Charge for FAT File System](#) – with lots of notes that the patents claimed are only about long filenames in FAT/FAT32
- The Register – [MS tightens IP grip on Cleartype and FAT- calls it liberalisation](#)
- CNET has a different spin – [Microsoft opens technology to more licensing](#)

## [Alternative Compensation for Music Workshop Today](#) [7:08 am]

I see that [Derek](#) and [Ed](#) are going to [Development of a Alternative Compensation System \(ACS\) for Digital Media in a Global Environment](#). Should be interesting to hear what comes of it. The perils of falling behind, this is the first I've heard of it – nothing like missing something going on under one's nose! (See also [Mary Hodder's post](#))

The meeting proposed by the Berkman Center will take place on December 5, 2003, from 8:00 a.m. – 5:00 p.m., in Cambridge, Massachusetts, USA, on the Harvard Law School campus. The meeting will have two broad segments: the morning will focus on a mandatory, state-run model; the afternoon will be devoted to consideration of a voluntary entertainment co-op model. The format will be a discussion led by Prof. Fisher.

[permalink to just this entry](#)

## [Alternative Compensation Meeting](#) [7:06 am]

I see that [Derek](#) and [Ed](#) are going to [Development of a Alternative Compensation System \(ACS\) for Digital Media in a Global Environment](#). Should be interesting to hear what comes of it.

The meeting proposed by the Berkman Center will take place on December 5, 2003, from 8:00 a.m. – 5:00 p.m., in Cambridge, Massachusetts, USA, on the Harvard Law School campus. The meeting will have two broad segments: the morning will focus on a mandatory, state-run model; the afternoon will be devoted to consideration of a voluntary entertainment co-op model. The format will be a discussion led by Prof. Fisher.

[permalink to just this entry](#)

## [A Lot of Boo-Hooing Over at USA Today....](#) [6:46 am]

(Sorry – No Boston *Globe* to read at breakfast today <G>)

Bemoaning the decline of the album format: [Downloading squeezes the art out of the album: A growing single-song culture is wiping out the multiple-track format](#) [pdf]. A *lot* of column-inches set aside, describing the return of the single as the leading edge of the end of music culture. Really.

The digital age, driven by single-song downloads, threatens to eradicate the multiple-track album, whether on compact disc, cassette or old-fashioned vinyl. It's not just the physical artifact that's joining shellac 78s, turntables and 8-track tapes in the pop graveyard: The very concept of songs integrated into a whole faces extinction.

[...] "The disappearance of the album as an entity would be sad, but anything to do with the evolution in how people access music excites me," singer Alanis Morissette says. "I'm very album-oriented, and my highest preference is that people experience my album as a whole, but I know people can gravitate to a certain song and listen to it ad nauseum. That's their right. It's about freedom of choice."

[...] Paid downloads, expected to reach \$80 million this year, \$1.1 billion next year and \$3.2 billion in 2008, account for a fraction of music sales but are expected to explode as Generation Y brings its entertainment dollars to the marketplace. While baby boomers maintained an allegiance to the album format as they graduated from vinyl to tape to CDs, the so-called echo boomers, a staggering 78 million of them, increasingly prefer the pay-per-tune route. And they favor shopping online over standing in line. In the week ending Sunday, downloaders bought 1.3 million tracks while stores sold 186,000 physical singles, according to Nielsen SoundScan.

[...] Joe Levy, music editor at *Rolling Stone*, theorizes that the CD has killed the album; that is, the arrival of the shiny digital disc with expanded room for sound helped push the concept of a bundled batch of songs toward extinction.

"The CD has been responsible for the death of the album in two ways," Levy says. "One is technology. Once music was sold in a digitized format, it could be easily traded on the Internet. CDs began to disappear as consumers collected music one MP3 at a time."

“The second factor is artistic. If you grew up with vinyl, you got 30 or 40 minutes on a record. Now you get 70 on a CD. The album format got swollen, unmanageable and, to some degree, unlistenable. Either you don’t have that much time to listen to it or the experience isn’t rewarding.”

Give me a break! When’s the last time you bought a pop CD that had more than 45 minutes of music? At least Dave Matthews gets it:

Dave Matthews sees the album’s demise as just another pothole in the music industry’s road to ruin.

“The real issue is that the technologies of how to access information have exploded, so everything the industry took for granted has been shattered, and now the industry has to get up and figure out how to deal with it,” he says. “The industry as it stands is going to be antiquated out of existence. And there’s no question we’ll work our way through it and become accustomed to something new.”

Or something that predates the recording industry: performing live. The album’s doom may be a boon not for singles but for the concert circuit.

“I don’t feel threatened financially by the collapse of the industry,” Matthews says. “The vast majority of my living is made from touring. Nobody’s going to be able to download that.”

But, striking a blow for the Paris Hilton Weltanschauung, we get Michelle Shocked:

Michelle Shocked considers the album’s downfall a another step toward a cultural wasteland. When she finished 1991’s *Arkansas Traveler*, an ambitious song cycle inspired by the blackface minstrel tradition, her label demanded she add a radio-friendly single. She dutifully delivered *Come a Long Way*.

“You can adapt to mundane things like marketing, but when the tail is wagging the dog and you generate singles for their own sake, you can pretty much kiss the concept album goodbye. That’s the direction labels are going in, because that’s where profit lies.”

Shocked refuses to dissect her 1988 breakthrough, *Short Sharp Shocked*, for track-by-track online sales. “I control the destiny of that album,” she says. “I own the rights so no label could chop it up and sell it on the Internet. If I did that, they’d only buy (hit single) *Anchorage*, which is only a part of that whole image. I refuse to be treated as a one-hit wonder.

“Trust me: We’re heading into a novelty song culture.”

Sorry, Michelle – get over yourself. You can create anything you want; but you shouldn’t expect me to sacrifice real technological advances, much less my own freedom to create and innovate (not to mention to elect *not* to buy your art), just to satisfy your artistic vision.

[permlink to just this entry](#)

## Thursday, December 4

### [Litman’s Latest](#) [9:32 am]

[Ernie points to](#) Jessica Litman’s latest, [Sharing and Stealing](#). I haven’t had a chance to read the paper yet (don’t ask what I came back to here at MIT – suffice it to say that an important NSF grant is now no longer being held up by an embarrassing oversight on my part!)

However, it’s interesting to read [Ernie’s comment](#), wherein he takes on one of the weakest points of the common P2P apologist’s argument – the claim that, if 60 million people are doing it, it must be right. He correctly points out that the issue with copyright is about something far more fundamental, and discussions that center on claiming that moral authority lies with the majority is just undermining the principled stand.

Ernie contends that "Copyright is about issues of culture and free speech." I’d suggest that there’s a third point – the connection between freedom and competitive markets. Jefferson’s famous copyright quote ("[It would be curious then, if an idea, the fugitive fermentation of an individual brain, could, of natural right, be claimed in exclusive and stable property](#)"), recall, emerges out of a larger debate about the merits of offering monopoly economic powers to creators (see this kuro5hin article to get some insight: [Thomas Jefferson, The DMCA,](#)

[Copyright, Fair Use, et al.](#)

As those who attended my recent lectures in the UK have been hearing, I have been working on showing how a large part of the problem of copyright emerges out of the fact that it is built upon two key compromises: trade-offs of that sacrifice (1) freedom of speech and (2) competitive markets in favor of (3) remunerating creativity. It's still too complicated a story to tell in a blog entry, but I'm working on it.

For 200 years, that compromise has worked out to the public's benefit, and for 200 years the incentives deriving from copyright have served to maintain a workable balance. However, today's copyright interests are so focused upon remunerating creativity that they are making choices/developing technologies/promoting legislation that are shifting the balance of those early compromises increasingly against the core freedoms upon which we rely.

Although some would argue otherwise, I do not believe that Jack Valenti and those of his ilk are actively pursuing a strategy to suppress our liberties. Rather, they are acting in accordance with the incentives we have set up for them – we have given them the monopoly that they are acting to protect and defend. But, those who are continuing to give them what they want are failing to recognize that each award in their favor is a blow to free speech and free market competition; and there is only so much resilience in the system before something will have to give.

[permalink to just this entry](#)

## [Michael Robertson \(and the Rest of Us\) Lose](#) [8:59 am]

[MP3.com archive is destroyed](#)

Michael Robertson's attempts to save the million-song music archive of the company he founded, MP3.com, appear to have been unsuccessful. The MP3.com domain was bought by CNET, and Vivendi Universal had warned that the plug would be pulled.

"I had no luck in buying the content, paying for the content to be backed up or facilitating a relationship with Archive.org," Robertson told us today in email. Robertson had met with Vivendi, and as we reported, Archive.org's Brewster Kahle was only too happy to host the content.

[...] "We're about to lose a museum filled with digital antiquities that are every bit as meaningful as their physical counterparts filling today's museums," Robertson had said.

[permalink to just this entry](#)

## [Plus ca change...](#) [8:42 am]

The Register: [Round 3: RIAA sues more file swappers](#); CNet News: [RIAA launches new file-swapping suits](#); Red Nova: [Music Industry Targets Even More Computerless](#)

The recording industry has filed 41 more lawsuits against computer users in at least 11 states it said were caught illegally distributing songs over the Internet, continuing its aggressive campaign against online music piracy.

[...] Among the RIAA's recent targets is retiree Ernest Brenot, 79, of Ridgefield, Wash., who wrote in a handwritten note to a federal judge that he does not own a computer nor can he operate one.

Brenot was accused of illegally offering for download 774 songs by artists including Vanilla Ice, U2, Creed, Linkin Park and Guns N' Roses.

Brenot's wife, Dorothy, said she and her husband were stunned by the claims, offended at the suggestion they listened to such music. Brenot was targeted in the previous round of 80 suits the recording organization filed late in October.

Brenot and her husband said their son-in-law briefly added Internet service to their own cable television account while living with the couple because Comcast Cable Communications Inc. said it would add a surcharge to send separate bills to the same mailing address.

"There's a mistake in this case," Dorothy Brenot said. "We're innocent in all of this, but I don't know how we're going to



prove it.”

[permalink to just this entry](#)

## Tuesday, December 2

### [Catching up....](#) [7:18 am]

Back from a long weekend in London following my teaching stint at Cambridge University, so it's going to be a little slow around here today — and I see from this morning's snow squall that I got back just in time for winter to start in *this* Cambridge, anyway....

I see from [Donna's site](#) that the Posner decision I briefly mentioned on Wednesday([A Setback for the Second Enclosure Movement](#)) is getting [considerable commentary out there](#).

[permalink to just this entry](#)

December 2003

**S M T W T F S**

[« Nov](#)      [Jan »](#)

1 [2](#) 3 [4](#) [5](#) [6](#)

[7](#) [8](#) [9](#) 10 [11](#) [12](#) 13

[14](#) [15](#) 16 [17](#) 18 [19](#) 20

[21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#)

[28](#) [29](#) [30](#) 31

- Legal Weblogs:
  - [Copyfight](#)
  - [Lawrence Lessig](#)
  - [GrepLaw](#)
  - [LawMeme](#)
  - [GrokLaw](#)
  - [Bag and Baggage](#)
  - [Ernie The Attorney](#)
  - [John Palfrey](#)
  - [Balkinization](#)
  - [Consensus at Lawyerpoint](#)
  - [beSpecific](#)
  - [The Importance of \(Being Ernest Miller\)](#)
  - [Dan Fingerman](#)
  - [Legal Theory Blog](#)
  - [LawGeek](#)
- Related Weblogs:
  - [Scrivener's Error](#)
  - [Super-DMCA](#)
  - [A Copyfighter's Musings](#)
  - [Tech Law Advisor](#)
  - [bIPlog](#)
  - [A blog doesn't need a clever name](#)
  - [The Shifted Librarian](#)
  - [Freedom to Tinker](#)
  - [Joho the Blog](#)
  - [Boing Boing](#)
  - [Doc Searls](#)

# Slashdot

News for Nerds. Stuff that matters.



## Login

[Why Login?](#)[Why Subscribe?](#)

## Sections

[Main](#)[Apache](#)[Apple](#)[1 more](#)[Askslashdot](#)[Books](#)[BSD](#)[Developers](#)[Games](#)[7 more](#)[Interviews](#)[Science](#)[1 more](#)[YRO](#)

## Help

[FAQ](#)[Bugs](#)

## Stories

[Old Stories](#)[Old Polls](#)[Topics](#)[Hall of Fame](#)[Submit Story](#)

## About

[Supporters](#)[Code](#)[Awards](#)

## Services

[Broadband](#)[Online Books](#)[Personals](#)[PriceGrabber](#)[Product News](#)[Tech Jobs](#)

## Officials secretly RFID'd at Internet Summit

Posted by [CmdrTaco](#) on Sun Dec 14, '03 10:40 AMfrom the [thats-just-creapy](#) dept.

[ewouenberg](#) writes "A [Washington Times article](#) reports that researchers managed to gain entrance to the Internet and technology conference in Switzerland last week only to discover that the summit's badges contained undisclosed RFID chips. The badges were handed out to more than 50 prime ministers, presidents and other high-level officials from 174 countries, including the United States."



## Slashdot Login

Nickname:

Password:

[\[ Create a new account \]](#)

## Related Links

- [ewouenberg](#)
- [Washington Times article](#)
- [More Privacy stories](#)
- [Also by CmdrTaco](#)

## Your Rights Online

- [Congress Loves Spam -- If It's From Congress](#)
- [MPAA Fights Pirates with Gentle Threats](#)
- [Court Rules Against Photographers in Copyright Suit](#)
- [DOJ Drops Online Music Antitrust Investigation](#)
- [Californians To Vote On Largest DNA Database](#)
- [The Year In Tech Law](#)
- [Liberal Party of Canada Sues Satire Website](#)
- [Linus Blasts SCO's Header Claims](#)
- [DeCSS: Jon Johansen Acquitted In Retrial](#)
- [Your Cell Phone Is Tracking You](#)

< [Walgreens PureDigital Camera Hacked](#) | [In Search of the Digital Uberdevice](#) >[Officials secretly RFID'd at Internet Summit](#) | [Log in/Create an Account](#) | [Top](#) | **216** comments | [Search Discussion](#)

Threshold:

**The Fine Print:** The following comments are owned by whoever posted them. We are not responsible for them in any way.**Cool.** (Score:5, Funny)by [torpor](#) (458) <[seclorumNO@SPAMmac.com](mailto:seclorumNO@SPAMmac.com)> on Sunday December 14, @ 10:42AM (#7716635)  
(<http://www.ampfea.org/> | Last Journal: [Saturday March 29, @01:33PM](#))

Politicians should be made to wear RFID's from the day they enter office in service of the public, to the day they leave that office.

"For the people, and of the people" can only be effective if the people keep a track on such people with power ...

**Re:Cool.** (Score:3, Interesting)by [Zebbers](#) (134389) on Sunday December 14, @ 11:22AM (#7717048)

umm

what use would the RFID be? it doesnt permit tracking a 'la gps...which would really be the only reason to take a 'politician'.

I despise the political system and politicians too...but that really isnt an insightful comment. A politician has a job, just like you. Should you be bagged and tagged to make sure you arent talking to competitors.

And besides whether we should...like I said, you must not understand RFID cause it would be useless to track people outside of a small, definitive area.

**Re:Cool.** (Score:3, Insightful)

by [torpor \(458\)](#) <[seclorumNO@SPAMmac.com](mailto:seclorumNO@SPAMmac.com)> on Sunday December 14, @11:30AM (#7717113)

(<http://www.ampfea.org/> | Last Journal: [Saturday March 29, @01:33PM](#))

*A politician has a job, just like you. Should you be bagged and tagged to make sure you arent talking to competitors.*

A politicians job is far more important than mine. It has its risks, it has its responsibilities.

Politicians should be held accountable for every single thing they do while they are on the job. Its the only way to ensure we -the people- don't get screwed ...

**Re:Cool.** (Score:5, Insightful)

by [ATMAvatar \(648864\)](#) on Sunday December 14, @12:22PM (#7717583)

(Last Journal: [Sunday September 28, @11:48AM](#))

Many people are closely monitored in the workplace. Why should politicians be any different?

**Re:Cool.** (Score:3, Interesting)

by [idlemachine \(732136\)](#) on Sunday December 14, @09:29PM (#7721507)

Apparently the Australian truth in advertising laws were modified to explicitly exclude politicians from being held accountable to them. Then again, they're also allowed to edit the \*official\* records of Parliamentary proceedings, just in case they ever stumble during a speech and actually reveal their true intentions. The more power and responsibility you have, the higher the level of accountability should be that comes with it. That we constantly absolve our politicians in this way just makes me think we're all fully aware that the way it is and the way we \*say\* it is are two completely different positions.

**Re:Cool.** (Score:2)

by [Syberghost \(10557\)](#) <[syberghostNO@SPAMeiv.com](mailto:syberghostNO@SPAMeiv.com)> on Monday December 15, @10:35AM (#7724731)

(<http://www.eiv.com/users/syberghost>)

Because killing or capturing you doesn't throw the entire country into chaos and endanger national security.

If anybody can monitor the President's location, that includes the bad guys.

**Re:Cool.** (Score:1)

by [telekon \(185072\)](#) on Sunday December 14, @01:15PM (#7718054)

(<http://www.nefac.net/> | Last Journal: [Monday December 15, @09:45AM](#))

*like I said, you must not understand RFID cause it would be useless to track people outside of a small, definitive area.*

Exactly. And that's why tagging politicians will be followed by confining all of them to a small, definitive area.

**Re:Cool.** (Score:2)

by [PReDiToR \(687141\)](#) on Sunday December 14, @05:05PM (#7719894)

(<http://preditor.is-a-geek.net/> | Last Journal: [Thursday August 14, @09:51PM](#))

God loves politicians, thats why Goatse was created for them ... The perfect place for them to feel at home in.

**Re:Cool.** (Score:4, Insightful)

by [Councilor Hart \(673770\)](#) on Sunday December 14, @11:41AM (#7717212)

They do have a private life, you know.

It is not our concern who they sleep with, eat with, talk to in their personal time.

It is not because they hold a public office, they don't have a right to privacy.

Everything that doesn't influence the execution of their mandate is not our concern, and should remain private.

Public life != Big Brother

**I agree** (Score:5, Insightful)by [mcc \(14761\)](#) <[amcclure@purdue.edu](mailto:amcclure@purdue.edu)> on Sunday December 14, @02:53PM (#7718863)  
(<http://allstarpowerup.com/>)

And I will gladly endorse that viewpoint just as soon as the same courtesy is extended to consumers and private citizens.

**Re:I agree** (Score:2, Interesting)by [Councilor Hart \(673770\)](#) on Sunday December 14, @03:35PM (#7719161)

Yes, privacy is an important issue. Don't (try to) violate mine, or I will go beserk.

Now, I defend this right for both parties because you can not expect that they uphold your right if you continually violate theirs.

By defending their rights, I am defending mine.

As to Clinton having an affair. I don't regard that as a cause for impeachment. That is a problem between him, his wife and his mistress. Thus a matter of his privacy.

On the other hand, he had an affair with a White House employee. That could be a ground for impeachment, if it compromises his ability to function as president.

The fact alone of having sex, with whomever is not sufficient cause.

**Re:I agree** (Score:1)by [Dick Faze \(711885\)](#) on Monday December 15, @10:30PM (#7731475)  
(Last Journal: [Wednesday October 01, @02:36PM](#))

Yes, use something that's wrong as justification for doing something wrong. That will make everything right.

**Re:Cool.** (Score:2)by [Kymerosst \(33885\)](#) on Sunday December 14, @04:48PM (#7719744)  
(Last Journal: [Friday August 22, @02:33PM](#))

*They do have a private life, you know.*

*It is not our concern who they sleep with, eat with, talk to in their personal time.*

*It is not because they hold a public office, they don't have a right to privacy.*

*Everything that doesn't influence the execution of their mandate is not our concern, and should remain private.*

*Public life != Big Brother*

*I think that's exactly the point the parent post was trying to make.*

*In other words, if politicians wouldn't want it, the people probably don't want it either.*

*A private citizen's life should remain private as well, and all talk of putting RFIDs on every single thing, including people, should be put to rest.*

**Michael Franti** (Score:2, Funny)by [Spectrum\\_Leap \(623660\)](#) on Sunday December 14, @08:10PM (#7721042)

"I don't give a stuff who they're screwing in private. I want to know who they're screwing in public!"

**I agree, but--** (Score:1)by [a24061 \(703202\)](#) on Monday December 15, @05:29AM (#7723408)

It's not their concern if private individuals want to use mind-altering substances or engage in unusual (but consensual) sexual practices in private. It's not their concern to monitor our e-mail, web browsing and library and bookstore records. So when they respect our rights to privacy, and only then, are they entitled to the same respect. And this principle should apply to employers as well as the state.

**Re:Cool.** (Score:2, Insightful)by [kommakazi \(610098\)](#) on Sunday December 14, @03:17PM (#7719047)

If Clinton "deserved" it like you say, why the hell is GWB still in office? He's outright lied and misled the public countless times about issues that *actually matter* and really do have a huge effect on the country and world at large. Yet there's not been any call for impeachment hearings...God the American public is fucking stupid.

**Re:Cool.** (Score:1)by [Scudsucker \(17617\)](#) on Sunday December 14, @04:18PM (#7719505)  
(<http://slashdot.org/>)

3.) *He lied under oath to a grand jury....that's why he was impeached...get it straight.*

Its debatable if he even lied, and even if he did lie, its not necessarily purgery. He said he "did not have sexual relations" with Monica.

sexual relations==euphamism for intercourse  
oral sex!=intercourse

So, at least in that statement, he wasn't lying. Splitting hairs yes, lying no.

But even if he did lie under oath, its not purgery if its not relevant. As his getting a BJ from Monica didn't have anything to do with the supposed harrasment against Paula Jones, it wasn't relevant.

**Re:Cool.** (Score:1, Offtopic)  
by [Kymermosst \(33885\)](#) on Sunday December 14, @05:00PM ([#7719852](#))  
(Last Journal: [Friday August 22, @02:33PM](#))

*Its debatable if he even lied, and even if he did lie, its not necessarily purgery. He said he "did not have sexual relations" with Monica.*

*sexual relations==euphamism for intercourse  
oral sex!=intercourse*

Bullshit. I've got a Webster's Dictionary sitting in front of me that was published before the Clinton administration.

sexual relations, 1. sexual intercourse; coitus. 2. any sexual activity between individuals. [1945-50]

You can't tell me that oral sex does not fall into number 2 there. Hence the word "sex" in the phrase.

*So, at least in that statement, he wasn't lying. Splitting hairs yes, lying no.*

Yes, he was, per my point above.

*But even if he did lie under oath, its not purgery if its not relevant. As his getting a BJ from Monica didn't have anything to do with the supposed harrasment against Paula Jones, it wasn't relevant.*

Go watch a a few trials sometime. It was absolutely relevent. It establishes a pattern of behavior where a powerful person is requesting (and sometimes getting) sexual favors from someone who is a lot less powerful.

We just had a case locally where a cop was getting BJs in return for not issuing tickets. (Again, power over powerless). Turns out there were over a dozen different women before one finally turned him in. I see very little difference between that and what Clinton was doing. It is not ethical to solicit sexual anything from someone in that relative position from you. Period.

How many women did Clinton really take advantage of using his positions as Governor and then President?

**Re:Cool.** (Score:2)  
by [Richard at work \(517087\)](#) \* on Sunday December 14, @05:52PM ([#7720241](#))  
(<http://www.coldfire.cx/>)

Clinton actually was very cunning here, as when he was asked this question, he requested that the Judge define exactly what "sexual relations" were. The definition that the judge gave precluded oral sex from the scope of the definition, so he was perfectly in his right to answer "I did not have sexual relations with that woman".

This is why he has never been tried for purjery, as he did not commit a crime by using the judges own definition.

**Re:Cool.** (Score:2, Informative)  
by [Scudsucker \(17617\)](#) on Sunday December 14, @06:22PM ([#7720419](#))  
(<http://slashdot.org/>)

*I've got a Webster's Dictionary sitting in front of me that was published before the Clinton administration.*

That's why its called splitting hairs, my friend. Some dictionary's have 50+ definitions of the word "set", does that mean I'm lying if I use it in one connotation, without mentioning the 49 others?

*Yes, he was, per my point above.*

No he wasn't, as the other poster proved.

*We just had a case locally where a cop was getting BJs in return for not issuing tickets. (Again, power over powerless). Turns out there were over a dozen different women before one finally turned him in. I see very little difference between that and what Clinton was doing.*

Except that all of those instances are illegal. Consensual sex with a person of age is not. As it wasn't an illegal act, and consensual sex is not harrassment, there was no purgery. And from all reports, its seems that Monica is the one who came onto Bill, not the other way around.

*How many women did Clinton really take advantage of using his positions as Governor and then President?*

Zero, probably. No, seriously, think about it for one single second. Congresss investigated him countless times. A couple of independant prosecutors investigated him with unlimited time, unlimited staff, unlimited budged, unlimited resources (the Starr investigation spent something like \$60 million alone). All these people went over every single spec of dust in Clinton's adult life with an electron microscope, **and the worst thing they can come up with is making misleading statements about their sex life?** Would **you** look as good after being investigated so throuarly? Would anyone? Hell, lets be fair and spend \$60 million frikkin dollars investigating every public official, starting with George Bush. Lets investigate his rumored cocaine use, the time he skipped out on his military service, the rumored abortion for a pregnant girlfriend, and his rumored shenanigans at various energy companies. All of those things are illegal; getting a BJ from a consenting adult is not.

*Bullshit.*

Eat it.

**facts** (Score:1)

by [Scudsucker \(17617\)](#) on Sunday December 14, @11:53PM (#7722298)

(<http://slashdot.org/>)

Fact: Republicans spent millions of dollars on many investigations of the Clintons.

Fact: The worst thing they could come up with was Bill fudging on his sex life.

Deal with it.

**Re:Cool.** (Score:2)

by [Dwonis \(52652\)](#) \* <[dlitz@dlitz.net](mailto:dlitz@dlitz.net)> on Sunday December 14, @10:08PM (#7721727)

(<http://www.dlitz.net/> | Last Journal: [Tuesday September 16, @12:22AM](#))

*So, at least in that statement, he wasn't lying. Splitting hairs yes, lying no.*

This is a weak argument. I don't care what words he used. He **communicated** untrue information, therefore, he lied.

However, since his sex life had nothing to do with his job as President, I think he's entitled to lie about it, because IMHO the question should not have been asked.

**Re:Cool.** (Score:2)

by [Maxwell'sSilverLART \(596756\)](#) on Sunday December 14, @11:54PM (#7722305)

(<http://www.barefootclown.net/>)

*I think he's entitled to lie about it, because IMHO the question should not have been asked.*

Not even as part of an investigation into allegations of *criminal rape* (see also: Juanita Broaderick)?

The question was legitimate. And, even if it isn't, you're not entitled to lie about it while under oath; the appropriate course of action would be to decline to answer. But, as I said, the whole sordid affair came about in due course of a rape investigation, and an investigation into Clinton's obstruction of same.

**Re:Cool.** (Score:1)by [Narchie Troll \(581273\)](#) on Monday December 15, @01:14AM (#7722625)

Wrong. It was the Paula Jones trial -- sexual harassment. Broadderick never even went to trial.

**Re:Cool.** (Score:1)by [Scudsucker \(17617\)](#) on Monday December 15, @12:01AM (#7722336)[\(http://slashdot.org/\)](http://slashdot.org/)

*He communicated untrue information, therefore, he lied.*

What part of oral sex not being intercourse is a misscommunication? There was no intercourse, so there was no lie.

And as Richard pointed out below:

Clinton actually was very cunning here, as when he was asked this question, he requested that the Judge define exactly what "sexual relations" were. The definition that the judge gave precluded oral sex from the scope of the definition, so he was perfectly in his right to answer "I did not have sexual relations with that woman".

**Re:Cool.** (Score:3, Interesting)by [gujo-odori \(473191\)](#) on Monday December 15, @12:09AM (#7722378)

*However, since his sex life had nothing to do with his job as President, I think he's entitled to lie about it, because IMHO the question should not have been asked.*

I'm a Republican, and did think the whole impeachment thing was a waste of everyone's time and money and shouldn't have been done. Richard Nixon took actions worthy of impeachment; Bill Clinton did not.

However, I don't think it's justifiable to say that what happened with Monica Lewinsky was his own business and he had a right to lie about it.

First of all, it happened in the oval office. If I had sex with someone on my employer's premises, whether it was during business hours or not, I assure you that they would take interest in that, would have a right to question me about it, and would most likely fire me. Therefore, you can't defend his lie by saying "It was his personal life, so he had a right to lie."

If it happend in the residence section of the Whitehouse, you might be able to make that claim, but since it happened in the oval office, it means he not only had sex on company premises, but he was on duty at the time. IIRC, he even made a phone call to some member of the House or Senate while he was getting knob schlobbed under the desk by Monica. That makes it very much the public's business, and I certainly think a letter of censure was in order. It's only impeachment that was a bit much.

**Re:Cool.** (Score:1)by [darkmeridian \(119044\)](#) on Wednesday December 17, @12:18AM (#7742587)

Clinton was sleeping with a government employee! That's illegal! Talk about hostile workplace environment!

But still, only one president before him has been impeached. There was a Republican effort to discredit him. Who hasn't had an affair? (Not to trivialize things, but we \*are\* talking about politicians, anyhow.)

**Re:Cool.** (Score:1)by [gujo-odori \(473191\)](#) on Wednesday December 17, @12:31AM (#7742643)

*That's illegal!*

I doubt it. Can you cite the law that says it's illegal for the president to sleep with a government employee? I don't know if interns are really considered government employees, but either way, I rather doubt that anything illegal took place. Their relationship was consensual, so to prove any illegality, you'd have to establish that he used his office to force her into a sexual relationship. Monica Lewinsky has made no such allegation, AFAIK, so it was consensual. It was wrong, and I'm sure his wife ripped him a new orifice, but he didn't break the law when he had an affair. He broke the law when he lied under oath.

Bonus question to the /. crowd, since you brought it up, who was the only president before him who was impeached, and why was he impeached?

Hint: !Watergate

**Re:Cool.** (Score:1)

by [FCAdcock \(531678\)](#) on Sunday December 14, @05:36PM (#7720131)

(<http://www.unsobersounds.com/> | Last Journal: [Thursday November 21, @02:05PM](#))

First off, she wasn't 18. Younger than him, maybe. but not 18. And anyways, 18's legal even if he's 95. Who cares what he did? The only thing that upsets me is that he lied about it. Had he told the truth I wouldn't have cared one bit. But it's still good to know that at least our president was getting some. He's got a stressful job. Lord knows that lady he married (and I use the term lady lightly), wasn't giving it up. I would pay for him a hooker if it keeps the stress from getting to him...

**Re:Cool.** (Score:1)

by [FCAdcock \(531678\)](#) on Sunday December 14, @05:41PM (#7720158)

(<http://www.unsobersounds.com/> | Last Journal: [Thursday November 21, @02:05PM](#))

Didn't you hear? When our military came and found him, he had a pistol in his possession. But seriously dude. He had thousands of his own citizens murdered. He had his own family members murdered. I may not like the idea of sending American men and women into a country where they are being shot at for political reasons, but I am glad that this man won't be able to hurt anyone any more. I was a strong supporter of Bush until he dropped the steel tariffs. Who cares about the war, he's selling off American Jobs and dosen't care. Forget overthrowing Hussen, Castro, or anyone else. I say we take back our White House and give it to someone who cares about American jobs.

**Re:Cool.** (Score:1, Offtopic)

by [Zapdos \(70654\)](#) on Sunday December 14, @11:53AM (#7717346)

Your idea is so dumb. There is this little thing called National Security.

Location matters not.

This would help get an elected official assassinated, perhaps their family and or children hurt.

**Re:Cool.** (Score:2, Insightful)

by [Politburo \(640618\)](#) on Sunday December 14, @12:08PM (#7717474)

Hi. Politicians are still citizens. They still have the rights we have. Sorry.

**Re:Cool.** (Score:2)

by [buckeyeguy \(525140\)](#) on Wednesday December 17, @04:05PM (#7748304)

(<http://slashdot.org/> | Last Journal: [Tuesday November 04, @07:02PM](#))

For every politician for whom that makes sense, there's at least one [Marion Barry](#) [rotten.com].

**Re:Cool.** (Score:3, Funny)

by [Handpaper \(566373\)](#) on Sunday December 14, @12:16PM (#7717540)

It's 01:30. Do you know where **your** Congressman is?

**Re:Cool.** (Score:2, Funny)

by [indianajones428 \(644219\)](#) on Sunday December 14, @05:35PM (#7720127)



It's 01:30. Do you know where your Congressman is?

Why, he's right there in my crosshairs...

Seriously, wouldn't this be too much of a security risk, even if it's just in one building and not everywhere they go?

**Re:Cool.** (Score:2)  
by [symbolic \(11752\)](#) on Sunday December 14, @12:27PM (#7717642)

If I had moderation points, I'd mod this up.

**Re:Cool.** (Score:2)  
by [t0ny \(590331\)](#) on Sunday December 14, @12:36PM (#7717715)

Wow, then all you need to do is find out how to detect RFIDs, and the time for psychotics to stalk and kill them would be drastically reduced.

What a well thought out idea!

**Re:Cool.** (Score:1)  
by [torpor \(458\)](#) <[seclorumNO@SPAMmac.com](mailto:seclorumNO@SPAMmac.com)> on Sunday December 14, @12:49PM (#7717822)  
(<http://www.ampfea.org/> | Last Journal: [Saturday March 29, @01:33PM](#))

If you've got the tech to make RFID work, you've got the tech to protect someone from thugs.

Duh.

**Re:Cool.** (Score:2)  
by [PReDiToR \(687141\)](#) on Sunday December 14, @05:08PM (#7719923)  
(<http://preditor.is-a-geek.net/> | Last Journal: [Thursday August 14, @09:51PM](#))

If they were so easily ID'd, wouldn't that encourage them to stop making choices about our lives that we felt justified murdering them over?

**Re:Cool.** (Score:2)  
by [t0ny \(590331\)](#) on Sunday December 14, @06:12PM (#7720361)

Why, who are you planning to murder?

**Re:Cool.** (Score:2)  
by [PReDiToR \(687141\)](#) on Sunday December 14, @11:10PM (#7722044)  
(<http://preditor.is-a-geek.net/> | Last Journal: [Thursday August 14, @09:51PM](#))

That Senator Hatch bastard could do with a good dose of syphilis or something equally nice.

Scuse me, but whenever I talk about killing prominent political figures over non-encrypted channels I like to mention words like terrorism, echelon, cocaine and nuclear.

**Re:Cool.** (Score:1)  
by [t0ny \(590331\)](#) on Monday December 15, @01:17PM (#7726474)

Wait patiently. Someone will be visiting you shortly.

**Re:Cool.** (Score:2)  
by [Zapdos \(70654\)](#) on Monday December 15, @07:08AM (#7723670)

Having politicians wear RFIDs is only useful to keep Texas Democrats from leaving the state.

Other than that it would present a personal danger to politicians and their families.

I guess the danger would outweigh the one benefit.  
Or are we short sighted?

**Re:Cool.** (Score:1)  
by [torpor \(458\)](#) <[seclorumNO@SPAMmac.com](mailto:seclorumNO@SPAMmac.com)> on Monday December 15, @08:03AM (#7723874)  
(<http://www.ampfea.org/> | Last Journal: [Saturday March 29, @01:33PM](#))

Why is their personal danger worth more than the combined danger of the populace being headed by people who are out of control?

**Re:Cool.** (Score:2)

by [Zapdos \(70654\)](#) on Monday December 15, @11:09AM (#7725073)

You have a GCECF.

(Gross Conceptual Error Carried Forward)

Knowing location does not provide any real form of control.

How would you exercise this control?

Are you going to send the police to arrest them?

Spank them?

You cant and wont.

Now for the first part, if you do not understand National Security.

Take President Bob (made-up) he has a wife and two lovely children. Someone uses the RFID to locate Bob they then take his wife and/or children hostage. They then tell Bob that his family will die if he vetos this bill or signs that bill.

**Re:Cool.** (Score:1)

by [torpor \(458\)](#) <[seclorumNO@SPAMmac.com](mailto:seclorumNO@SPAMmac.com)> on Monday December 15, @01:34PM (#7726629)

(<http://www.ampfea.org/> | Last Journal: [Saturday March 29, @01:33PM](#))

yeah, okay ... 'theoretical scenario vs. theoretical scenario' ... President Shrub goes to China for a secret meeting with his masters, how you gonna know if that happens, eh?

Look, it was a half-assed jest in the beginning, now its a half-assed argument.

**They Got Him!** (Score:5, Funny)

by [bruthasj \(175228\)](#) <[bruthasj@@@yahoo...com](mailto:bruthasj@@@yahoo...com)> on Sunday December 14, @10:43AM (#7716637)

(<http://www.geocities.com/bruthasj> | Last Journal: [Monday August 04, @07:17PM](#))

With RFID.

Note for the humor-impaired: this is a joke.

**Re:They Got Him!** (Score:2, Funny)

by Anonymous Coward on Sunday December 14, @10:50AM (#7716734)

Well, one can hope that Ossama bin Laden got to this conference too. It might help the CIA to get him too ;o)

**Re:They Got Him!** (Score:1)

by [Moth7 \(699815\)](#) on Sunday December 14, @11:01AM (#7716835)

As incompetent as the US may be, I doubt that RFIDing him would be their first priority if they found him ;)

**DUPE!!** (Score:2, Informative)

by Anonymous Coward on Sunday December 14, @10:43AM (#7716641)

[http://slashdot.org/article.pl?sid=03/12/12/002825\\_6&mode=nested&tid=126&tid=158&tid=172&tid=99](http://slashdot.org/article.pl?sid=03/12/12/002825_6&mode=nested&tid=126&tid=158&tid=172&tid=99) [slashdot.org]

**Are Dups Bad?** (Score:2)

by [G4from128k \(686170\)](#) on Sunday December 14, @11:13AM (#7716964)

Dups provide a chance to post additional insights that emerge from the original story. I find that reading all the +5 comments from the first posting of the story provides more food for thought once the dup appears.

**New terrorist spying method** (Score:5, Funny)

by [brian728s \(666853\)](#) on Sunday December 14, @10:44AM (#7716653)

Lightbulbs are now being labeled a terrorist device, used to spy on people and documents at places including the pentagon, the whitehouse, and even the United Nations building. Hackers used the light bulbs to send out light, which when intercepted by their illegal hacker tools called "eyes", can identify diplomats, and read classified documents. Americans can rest assured that their safety is being protected by operation "hammerbulb". Democrats are concerned about a lack of hammers to complete the operation, but administration officials assure them that rocks can be used if the shortage proves true.

**Re:MOD PARENT SIDEWAYS** (Score:1, Funny)  
by Anonymous Coward on Sunday December 14, @02:40PM ([#7718767](#))

Mod parent +2i because the real directions are taken.

**Privacy** (Score:5, Funny)  
by [penguinoiD \(724646\)](#) <[spambait001@yahoo.com](mailto:spambait001@yahoo.com)> on Sunday December 14, @10:44AM ([#7716654](#))  
(Last Journal: [Sunday December 14, @10:53AM](#))

They met to discuss privacy matters on the internet (among other things).  
I wonder what their policy will be?

**Re:Privacy** (Score:1)  
by [daminotaur \(732705\)](#) on Sunday December 14, @01:16PM ([#7718068](#))

The RFID flap is the most interesting thing to come out of WSIS. And even it's pretty lame. Don't worry about ANY policy coming out of this group. I went to their web site <http://www.itu.int/wsis/> the other day and subjected myself to a lot of their streaming video. First off, it was almost all politicians--can you say vacuous platitudes? Boring as hell, and they were all saying the same thing: "Information should be FREE for all the oppressed peoples of the world, kumbaya." If they weren't politicians they were NGO types. Basically a series of three-minute hates against the US as the 800-pound gorilla of the internet--they were polite enough not to mention the US by name usually, but that was the subtext. Bunch of utopian dreamers. Since when has ANYTHING been free? The little problem of IP rights was hardly even mentioned, only by the Iranian president briefly. He used the amusing phrase "Network Order" to describe US hegemony, a play on "New World Order"

**duplicate** (Score:1, Informative)  
by [hugesmile \(587771\)](#) on Sunday December 14, @10:45AM ([#7716663](#))

Wasn't this [already discussed?](#) [slashdot.org]

**Slashdort Needs to RFID Its Postings** (Score:1, Redundant)  
by [aheath \(628369\)](#) \* <[adam.heath@comcast.net](mailto:adam.heath@comcast.net)> on Sunday December 14, @10:46AM ([#7716682](#))

For those of you who are experiencing the sensation of "deja vu all over again" please see [WSIS Physical Security Cracked](#). [slashdot.org]

**Welcome Welcome to to Slashdot Slashdot** (Score:3, Redundant)  
by [Doc Ruby \(173196\)](#) on Sunday December 14, @10:47AM ([#7716688](#))

I know the Slashdot editors don't read the story submissions, because my earthshattering submissions are never accepted. But do they even read [the Slashdot homepage](#) [slashdot.org]? They might notice [duplicate stories](#) [slashdot.org].

**from the department of redundancy department** (Score:2)  
by [Doc Ruby \(173196\)](#) on Sunday December 14, @11:22AM ([#7717049](#))

The Slashcode already extracts URLs from stories into sidebars. Why not a revision that compares those URLs in a submission to those in past submissions? Then editors can see whether a submission is a dup as they go through their incoming queue.

**Re:from the department of redundancy department** (Score:2)  
by [The Cydonian \(603441\)](#) on Sunday December 14, @11:53AM ([#7717347](#))  
(Last Journal: [Tuesday December 16, @12:21AM](#))

As you can see from this case itself, your solution *wouldn't* have caught this dupe. The earlier link was from a press release, while this one's from Washington Times.

Still, /. editors could have acknowledged the earlier story before posting it to the front page.

**Re:Welcome Welcome to to Slashdot Slashdot** (Score:1)  
by [MooseGuy529 \(578473\)](#) <[ten.knilhtrae.ta.elttuTsamohT](mailto:ten.knilhtrae.ta.elttuTsamohT)> on Sunday December 14, @12:06PM ([#7717456](#))  
(<http://www.slashdot.org/~MooseGuy529/journal> | Last Journal: [Friday March 28, @08:29PM](#))

I'll bet it would be possible to use a spam-filter-esque system to compare the text of the articles and the links they point to. By weighting heavily the text of the links and the headings in the linked documents, they could give stories a dup-score and the editors would be shown a list sorted from highest-to-lowest.

Wait... it would have to have a limit on the number of stories it goes back, or else it will compare this one story to every other story in the database! Any ideas?

**Bayesian filter for articles?** (Score:2)by [Doc Ruby \(173196\)](#) on Sunday December 14, @12:18PM (#7717551)

The filter must compare the submission to every article, or the omitted archives might contain dup's. Why not? How about a Bayesian filter? How about a hash of the "salient" details against which a dup would match?

**Re:Welcome Welcome to to Slashdot Slashdot** (Score:3, Funny)by [1u3hr \(530656\)](#) on Sunday December 14, @12:46PM (#7717803)

*I'll bet it would be possible to use a spam-filter-esque system to compare the text of the articles....*

I bet it would be possible to check the spelling of the articles posted using a "spell checker". I recall using one in the late 70s on my student Unix system.

**Re:Welcome Welcome to to Slashdot Slashdot** (Score:3, Informative)by [maelstrom \(638\)](#) \* on Sunday December 14, @12:19PM (#7717561)(<http://signalnine.com/> | Last Journal: [Thursday March 07, @10:39PM](#))

CmdrTaco hasn't read this site in years.

**Re:Welcome Welcome to to Slashdot Slashdot** (Score:2)by [shdragon \(1797\)](#) \* on Monday December 15, @10:36AM (#7724742)(<http://127.0.0.1/> | Last Journal: [Saturday July 26, @10:40AM](#))

Sometimes, I can't say I blame him.

**Re:Welcome Welcome to to Slashdot Slashdot** (Score:1)by [damien\\_kane \(519267\)](#) <[damien.strat@net](mailto:damien.strat@net)> on Sunday December 14, @12:34PM (#7717701)(<http://damien.dhs.org/>)

*They might notice duplicate stories.*

I would think you're new here... but since you've got a low UID, you're just hijacking your faters /. account, right? All the little slashbots around have to realize, dupes will never disappear. Taco doesn't want to code a dupe-finder, and the editors just don't care.

**Re:Welcome Welcome to to Slashdot Slashdot** (Score:2)by [Tim C \(15259\)](#) on Sunday December 14, @12:42PM (#7717769)

*I would think you're new here... but since you've got a low UID*

173196 low? That's a joke, right? ;-)

For what (little) it's worth, the problem is getting worse. A few years ago, when I was new here, there was hardly ever a dupe. As the site's grown, though, and I suppose the number of submissions has increased, they've started slipping through more and more often.

I wouldn't say it's a huge problem - after all, just because something's been discussed before doesn't stop us all discussing it again (eg Windows vs Linux, RIAA/MPAA vs the world, etc). I would have thought, though, that it would be fairly easy to search for recently-posted stories based on keywords from the submission under consideration... Maybe they do do that, though, and there're just so many that it'd be almost impossible not to miss one occasionally. After all, even if you only mess up one time in a hundred, as you increase the number of times you do something, you'll increase the number of mistakes you make.

**DIY** (Score:2)by [Doc Ruby \(173196\)](#) on Sunday December 14, @01:00PM (#7717912)

I've been reading dup's on Slashdot since 1998, although my current UID dates from later. Help me write a dup-matcher filter for the editors' submissions queue, and we can help do something about it. The Slashcode is OSS, so we can back up our complaints with constructive solutions by patching the code.

**Re:Welcome Welcome to to Slashdot Slashdot** (Score:1, Redundant)by [Doc Ruby \(173196\)](#) on Sunday December 14, @11:15AM (#7716987)

Don't let redundancy stop you from posting a comment.

**perfectly perfect** (Score:2)by [Doc Ruby \(173196\)](#) on Sunday December 14, @12:01PM (#7717421)

**"Re:Welcome Welcome to to Slashdot Slashdot (Score:1, Redundant)"**

**Re: Welcome Welcome to to Slashdot Slashdot** (Score:1)

by [FCAdcock \(531678\)](#) on Sunday December 14, @05:50PM (#7720219)

(<http://www.unsobersounds.com/> | Last Journal: [Thursday November 21, @02:05PM](#))

exactly, I never let redundancy stop me from posting a comment.

**Re: Welcome Welcome to to Slashdot Slashdot** (Score:1, Redundant)

by [Doc Ruby \(173196\)](#) on Sunday December 14, @11:20AM (#7717022)

Don't let "redundancy" stop you from posting a comment.

**We don't need no stinkin badges!** (Score:3, Funny)

by Anonymous Coward on Sunday December 14, @10:48AM (#7716704)

Badges? We don't need no stinkin badges!

**Re: We don't need no stinkin badges!** (Score:2)

by [pipingguy \(566974\)](#) <[pbowers AT pipingdesign DOT com](mailto:pbowers AT pipingdesign DOT com)> on Sunday December 14, @07:46PM (#7720885)

(<http://www.pipingdesign.org/>)

*Badges? We don't need no stinkin badges!*

I, for one, am getting fed up about the continued misspelling in this famous quote. It's "steenking".

**Re: We don't need no stinkin badges!** (Score:2)

by [1u3hr \(530656\)](#) on Monday December 15, @12:10AM (#7722390)

*Badges? We don't need no stinkin badges!*

*I, for one, am getting fed up about the continued misspelling in this famous quote. It's "steenking".*

From [the Stinking Badges](#) [darryl.com] home page:

*The Treasure of The Sierra Madre, ((C) 1935) by B. Traven*

*"Badges, to god-damned hell with badges! We have no badges. In fact, we don't need badges. I don't have to show you any stinking badges, you god-damned cabron and ching' tu madre!"*

There's a [sound clip from the 1948 movie](#) [darryl.com] on that page, and that doesn't sound like "steenking" either.

**Re: We don't need no stinkin badges!** (Score:1)

by [celery stalk \(617764\)](#) on Monday December 15, @02:11AM (#7722846)

It's possible they might be referring to the *Blazing Saddles* reference.

**Re: We don't need no stinkin badges!** (Score:2)

by [pipingguy \(566974\)](#) <[pbowers AT pipingdesign DOT com](mailto:pbowers AT pipingdesign DOT com)> on Monday December 15, @11:37AM (#7725417)

(<http://www.pipingdesign.org/>)

*It's possible they might be referring to the Blazing Saddles reference.*

That, and WKRP. Nice job of tracking down the apparent original source by 1u3hr.

**Re: We don't need no stinkin badges!** (Score:1)

by [kommakazi \(610098\)](#) on Sunday December 14, @03:24PM (#7719092)

No, the comment isn't the dupe, it's just you.

**Re: We don't need no stinkin badges!** (Score:2)

by [Dwonis \(52652\)](#) \* <[dlitz@dlitz.net](mailto:dlitz@dlitz.net)> on Sunday December 14, @10:14PM (#7721756)

(<http://www.dlitz.net/> | Last Journal: [Tuesday September 16, @12:22AM](#))

"This comment is a dupe.' is a dupe." is not a dupe.

**Good.** (Score:5, Insightful)

by [Space cowboy \(13680\)](#) <[slashdot.gornall@net](mailto:slashdot.gornall@net)> on Sunday December 14, @10:50AM (#7716738)

(<http://hostip.info/>)

I hope the media catch hold of it and hype it to hell and beyond. Get some high-flying politico commentators saying how they should have been informed.

Understanding about fire being hot often comes after one has been burnt. Perhaps they'll feel that they shouldn't be "spied on" without their knowledge. Perhaps it might influence decisions they make in future...

Simon.

**Re:Good.** (Score:3, Insightful)

by [JohnnyBigodes \(609498\)](#) <[blueroom AT digitalmente DOT net](mailto:blueroom AT digitalmente DOT net)> on Sunday December 14, @11:02AM (#7716861)

Good luck.. they (the politicians) will mostly complain about THEIR privacy, citing matters of national security. The people's privacy will always be watched in some way or another due to the need of "a general well-being".

**And watch ...** (Score:2, Insightful)

by [Lead Butthead \(321013\)](#) on Sunday December 14, @01:39PM (#7718266)

how quickly they will forget and proceed to do on to their citizens what they complain loudly of.

**watching you watch me** (Score:5, Insightful)

by [segment \(695309\)](#) <[sil@infiltrat\[ \]net \['ed.' in gap\]](mailto:sil@infiltrat[ ]net ['ed.' in gap])> on Sunday December 14, @10:51AM (#7716741) (<http://www.scumgroup.com/>)

Washington Post has their own agendas politically when it comes to reporting. Sure it's pretty shitty to be monitored, but there is nothing stating that any information used was used for anything other than maybe for the sake of having some card manufacturers new card being tested.

Remember intelligence agencies from all over the place keep tabs on each other via other means (ECHELON, HUMINT, OSINT, IMINT, SIGNIT), so I doubt this was anything to be concerned with. Strictly something `chick' to report on. It's far more easier to set up assets to bang (screw/lay/fsck) one of these guys for info, than it would to keep watch of what they do.

User gets in car to go to summit, user's Eazypass or other form of cardpaymentsys tracks what exits he uses via tolls paid. User stops at gasoline station, credit card is used, card information is transmitted. User talks the beltway, cameras capture this. Get the picture? Everyone else sure did. Again other than this being all the rage (RFID's) I doubt it was something major, but surely someone with agendas sees it to be so. When they can produce something absolute that was used with this information, not just 'oh my look at this an RFID story' than I'll worry.

PS... Proof doesn't mean `hey we're the Foobar Newspaper

**Re:watching you watch me** (Score:3, Informative)

by [grondu \(239962\)](#) on Sunday December 14, @10:57AM (#7716809)

*Washington Post has their own agendas politically when it comes to reporting.*

The link is to the Washington *Times* , not the Washington Post.

**Re:watching you watch me** (Score:2)

by [segment \(695309\)](#) <[sil@infiltrat\[ \]net \['ed.' in gap\]](mailto:sil@infiltrat[ ]net ['ed.' in gap])> on Sunday December 14, @11:04AM (#7716877) (<http://www.scumgroup.com/>)

shit i need to wake up... thanx and doh! but in essence there still isnt anything more than some rfid bs... And I should have known it was the times because of the ugly ass colors they use

**Re:watching you watch me** (Score:1)

by [Orne \(144925\)](#) on Sunday December 14, @02:05PM (#7718478) (<http://www.geocities.com/polysillycon>)

That doesn't make the post any less true.

The Washington Post makes up stories with left-wing sping, the Washington Times makes up stories with left-wing sping. Its up to the consumer to buy the version that they feel best represents the truth.

**Washington Times != left-wing** (Score:2)

by [jdfox \(74524\)](#) on Sunday December 14, @06:38PM (#7720498)

The Washington Times is owned by the Unification Church, also known as the "Moonies". They are quite right-wing, even by US standards.

The Moonies now also own the once-great United Press International, UPI. Just about all the good journalists left UPI in disgust when the takeover happened a few years back, and it turned into a sort of National Enquirer Newsfeed, practically overnight.

**Re: watching you watch me** (Score:1)

by [kommakazi \(610098\)](#) on Sunday December 14, @03:31PM (#7719142)

*Strictly something `chick' to report on.*

I think the word you're looking for is 'chic.

**Summary** (Score:4, Interesting)

by [FTL \(112112\)](#) \* [<slashdot@NOSPam.neil.fraser.name>](mailto:slashdot@NOSPam.neil.fraser.name) on Sunday December 14, @10:53AM (#7716763) (<http://neil.fraser.name/>)

To summarise the article, a group of reporters were pissed that they weren't invited to attend the conference. They dissected a security card, and found (shock, horror) that it contained features designed to maintain security at said conference. Since this is the only dirt they managed to find, they spin it up into a sky-is-falling end-of-the-world privacy story.

I'd have a lot more respect for activist reporters if they would report the facts without hype. It's not the second coming, it's possibly a minor infraction of the Swiss information laws.

**Re:Summary** (Score:5, Funny)

by [Crash Culligan \(227354\)](#) on Sunday December 14, @11:47AM (#7717267)

(<http://skipjack.bluecrab.org/~dwood/> | Last Journal: [Friday October 24, @12:28PM](#))

*To summarise the article, a group of reporters were pissed that they weren't invited to attend the conference.*

That's no surprise. If I recall correctly, the G7 summits are intended to be discussions on global economic policy, to which none of the affected people (pretty much everybody but government officials) are ever invited. (In fact, I don't hear of many economists going to those conferences either; if I'm wrong, please correct.)

As for press not getting in, sure you may loathe muckraker reporting (many people do), but sometimes there's just too much muck to allow to pile up. Do you *really* want your government to be deciding elements of policy without any input from its constituency? That's becoming the norm, and guerilla reporting may soon be the *only* way the operation of said government can come to light.

*They dissected a security card, and found (shock, horror) that it contained features designed to maintain security at said conference. Since this is the only dirt they managed to find, they spin it up into a sky-is-falling end-of-the-world privacy story.*

Yeah, I see where the article *could* sound like sour grapes. But then there's something to be said for the irony of the situation, and I'm glad that *someone* was in there to highlight it.

1. Government officials attend privacy and security conference.
2. Reporters crash privacy and security conference, demonstrating lack of security.
3. Reporters analyze badges from privacy and not-security conference and find RFID tags, demonstrating lack of privacy.
4. Article about lack-of-privacy and not-security conference reaches the public.
5. ???
6. **Privacy!!**

I'm not *perfectly* sure, but I think that next-to-the-last step should be *Citizens of the world slap their respective governments upside the head and scream "What were you goobers THINKING??"*

At least, that's my take on it...

**Re:Summary** (Score:1)by [kommakazi \(610098\)](#) on Sunday December 14, @03:33PM (#7719155)

lol!

mod parent up!

**Re:Summary** (Score:5, Insightful)by [Ironica \(124657\)](#) on Sunday December 14, @12:56PM (#7717881)(Last Journal: [Monday November 10, @03:50PM](#))*a group of reporters were pissed that they weren't invited to attend the conference.*

And from the article, there's no indication that they're the same as the group of researchers who snuck in.

*They disected a security card, and found (shock, horror) that it contained features designed to maintain security at said conference.*

If that's what it was for, how come the security people couldn't tell them that? I'm glad you were able to get more info out of them than the researchers were.

*Since this is the only dirt they managed to find, they spin it up into a sky-is-falling end-of-the-world privacy story.*

The fact that they faked their way in so easily was the first bit of dirt they dug up. The fact that there were undisclosed monitoring devices in the badges was the next. The final blow was that they couldn't get any info from security about the monitoring, and basically that the conference violated at least three privacy laws in the current jurisdiction.

And that if this is how it goes in Switzerland, how will things go in Tunisia next year?

If you figure it's no biggie, maybe you're right. But then again, if we send a bunch of prime ministers and other politicians to all congregate in a single place, and then we put tags on them so that we know their comings and goings, and who is talking with whom, and then we don't have any apparent plan to purge that info at any point... how easy will it be for every terrorist in the world to strike against their least favorite government at next year's conference? This seems vaguely important to me.

**Countermeasures** (Score:5, Interesting)by [G4from128k \(686170\)](#) on Sunday December 14, @10:53AM (#7716764)I wonder if someone is goign to make a killing by selling little RFID chip & reader detectors. Richard Stallman suggested [RFID detectors and destroyers](#) [rfidprivacy.org] as a challenge for privacy adocates. Perhaps clothing with conductive/dissapative threads will be the next fashion trend (just don't count on your cellphone ringing if its inside your pocket ;)).**Re:Countermeasures** (Score:3, Funny)by [SurgeonGeneral \(212572\)](#) on Sunday December 14, @10:59AM (#7716821)(Last Journal: [Tuesday February 11, @06:42PM](#))

Well how about just some way I can find my keys and television remote control.. That alone would make this technology the best thing since sliced silicon.

**Re:Countermeasures** (Score:2)by [Ironica \(124657\)](#) on Sunday December 14, @01:10PM (#7718002)(Last Journal: [Monday November 10, @03:50PM](#))*Well how about just some way I can find my keys and television remote control.. That alone would make this technology the best thing since sliced silicon.*[Here you go.](#) [sharperimage.com]**Re:Countermeasures** (Score:1)by [dreadknight \(324674\)](#) on Sunday December 14, @01:22PM (#7718114)

I wonder if anybody has thought of making an RFID chip that just throws out static interference, thus drowning out any useful information that a real RFID chip would give...

**Re:Countermeasures** (Score:1)by [kommakazi \(610098\)](#) on Sunday December 14, @03:37PM (#7719175)

Quick! Everyone get your aluminum foil hats...and shirts...and pants...hell just make a full body suit out of it...



**Re: Microwave** (Score:2)

by [bill\\_mcgonigle \(4333\)](#) \* on Monday December 15, @02:00PM (#7726902)  
(<http://www.zettabyte.net/> | Last Journal: [Tuesday October 28, @02:20PM](#))

Shhh, you'll ruin my plan to resell \$70 microwaves from BJ's for \$499 as RFID de-programmers. :)

**Privacy issue, or planning aid?** (Score:2, Interesting)

by [xplenumx \(703804\)](#) on Sunday December 14, @11:01AM (#7716848)  
(Last Journal: [Monday September 08, @10:38PM](#))

I would think that the information provided by the RFID tags would be invaluable - not in terms of violating privacy but for the planning of future conferences. I'd gladly wear RFID chips in my conference badge if it lead to improved trafficking for future conferences. One doesn't attend conferences for the privacy.

**Re: Privacy issue, or planning aid?** (Score:4, Insightful)

by [Dashing Leech \(688077\)](#) on Sunday December 14, @11:34AM (#7717155)

*One doesn't attend conferences for the privacy.*

So, if you spent 2 hours in the bathroom with bad diarrhea, you'd have no problem telling them if they asked you why you were in there for so long and why you missed a few sessions? Is that it, every minute of your day there is open for anyone's scrutiny? (That is, anyone with access to an RFID tracker.)

**Re: Privacy issue, or planning aid?** (Score:1, Funny)

by Anonymous Coward on Sunday December 14, @11:50AM (#7717311)

Well i'd rather tell them i had a bad case of Diarrhoea then tell them that I was doing the wife of (insert name of desired country) in it.

**Re: Privacy issue, or planning aid?** (Score:2)

by [Viceice \(462967\)](#) on Sunday December 14, @12:01PM (#7717422)

Well i'd rather tell them i had a bad case of Diarrhoea then tell them that I was doing the wife of the president/prime minister of (insert name of desired country) in it.

**Re: Privacy issue, or planning aid?** (Score:2)

by [Dashing Leech \(688077\)](#) on Sunday December 14, @04:43PM (#7719704)

I'd rather they keep their nose out of my business. Actually, if it was bad diarrhea, maybe they should be forced to stick their nose in my business.

**Hmm, just maybe...** (Score:1, Redundant)

by [11223 \(201561\)](#) on Sunday December 14, @11:02AM (#7716859)

Perhaps if they RFID-tagged Slashdot submissions, they could detect dups at a distance, before they were posted.

**Creapy?** (Score:1, Insightful)

by Anonymous Coward on Sunday December 14, @11:20AM (#7717025)

Creepy. It's just CREEPY. I am not sure Creapy is even a word. Jeez.

**Creapy?** (Score:1)

by [dstillz \(704959\)](#) on Sunday December 14, @11:20AM (#7717029)  
(<http://www.derikstiller.com/> | Last Journal: [Friday October 03, @08:45PM](#))

From the that's-just-crappy dept, with an apostrophe.

**Washington Times** (Score:1)

by [LittleDan \(669174\)](#) on Sunday December 14, @11:24AM (#7717064)

We should take this with a grain of salt; this is the Washington Times we're dealing with. They have a history of making up news stories. I wouldn't trust them.

**Re: Washington Times** (Score:4, Interesting)

by [canajin56 \(660655\)](#) on Sunday December 14, @01:53PM (#7718389)

Everybody makes up news stories. Like when NBC needed to show that GM trucks explode when struck from the side. They said the fuel tank ruptured. But what they did was overfill the gas tank, didn't screw the gas cap on (Just left it sitting on top) and then they strapped remotely detonated explosive under the truck to ignite the gas when it spilt out! And even then, the flames went out after a few seconds, so they had to "creatively" edit it to make the fire look worse. Here is a [summary](#) [whatreallyhappened.com] Although he did get one thing wrong: NBC hasn't died yet, in the 4 years since it happened. Hmm, I also recall something about slowing down the tape, so it looked like the truck they hit it with was going fairly slow, but it was actually going really fast.

**oh no! we know now...** (Score:3, Funny)by [Zed2K \(313037\)](#) on Sunday December 14, @11:57AM (#7717382)

That someone hit the bathroom at 12:30pm and then again at 3:30pm. They also exited the room for a smoke break after their bathroom break. Oh and don't forget the super secret buying of a Snickers bar at 3:35pm.

**WTF, Over...** (Score:5, Insightful)by [Sylver Dragon \(445237\)](#) on Sunday December 14, @12:00PM (#7717412)[\(http://www.dragon-tech.net/](http://www.dragon-tech.net/) | Last Journal: [Tuesday December 02, @02:57PM](#))

Maybe its just me, but this seems like a whole lot of noise over nothing. Those badges were probably security badges. You know, the kind many of us corporate workers wear every day to work. If you are one of those workers who have to swipe your ID badge in front of a little box that goes *beep*, and an LED turns green, and the door opens, the you are carrying an RFID tag (possibly even a smart card, but this is not as common). This is no big deal, its simply a way to control access. Technically, it provides some employee tracking, but its also very useful for security. Heck, even parking garages are using these for employees now. My girlfriend has a little card (HID Prox card), which she uses at work to get into and out of the parking complex for work. Myself, I work at a company that builds physical security systems, so I work with these things every day. And, I find, that most of the privacy concerns are **way** overblown. Though, I still don't like the idea of carrying one on me, I am a bit of a privacy nut afterall. If anything, this article sounds like a bunch of reporters got pissed, because they weren't allowed into a closed door conference, and broke the rules to get an access badge, and then reported on the *evil* RFID tag in the card, despite this being a very common thing, especially in places where security is an issue.

**Hipocrisy?** (Score:2, Insightful)by [InfiniteWisdom \(530090\)](#) on Sunday December 14, @12:14PM (#7717516)[\(http://www.vinaypai.com/\)](http://www.vinaypai.com/)

RFID concerns are overblown, except when the tags are on YOU.

**Re:Hipocrisy?** (Score:4, Insightful)by [Sylver Dragon \(445237\)](#) on Sunday December 14, @12:34PM (#7717699)[\(http://www.dragon-tech.net/](http://www.dragon-tech.net/) | Last Journal: [Tuesday December 02, @02:57PM](#))

No, RFID concers are overblown. I just happen to be one of the people that believes in erring on the side of caution. Truth is, those little suckers take some good sized equipment to read from any worthwhile distance, so carrying my work ID badge on me at all times (I just keep it in my wallet) really isn't a cause for concern. What bothers me, is the idea of any government of corporation trying to hide these things on me, so that they can track me when the technology advances far enough for the readers to be small and have good range. Also, note that I did say privacy **nut**, which usually implies being irrational. Which many of my fears about privacy are, but I'll hang onto them, just in case one of them is right.

**Re:Hipocrisy?** (Score:1)by [InfiniteWisdom \(530090\)](#) on Sunday December 14, @02:11PM (#7718525)[\(http://www.vinaypai.com/\)](http://www.vinaypai.com/)

How hard is it to hide an RFID detector in a doorframe? Or a newspaper stand on a street corner or under the sidewalk for that matter. To me the key concerns are that

- a) Unlike UPC codes, RFID tags will identify a specific instance of an item. Its not just a copy of "Applied Cryptography" but the specific copy of Applied Cryptography that I bought.
- b) RFID tags will probably be built into the manufacturing process and hard or impossible to remove or disable.

Imagine the invasive marketing that will be possible! Imagine the excesses that overzealous law enforcement will be capable of.

**Re:Hipocrisy?** (Score:1)by [uarch \(637449\)](#) on Sunday December 14, @05:54PM (#7720253)

If you're really worried about someone identifying your specific copy of "Applied Cryptography" just microwave the thing.

The induced current will fry any RFID in the thing.

Sure, this may not be the best way to remove an RFID tag from your next cellphone but it'll work on a lot of things.

**Re:Hipocrisy?** (Score:1)

by [InfiniteWisdom \(530090\)](#) on Sunday December 14, @07:36PM (#7720834)  
(<http://www.vinaypai.com/>)

Several people have suggested that microwaving RFID tags can cause them to burst into flames

**Re:WTF, Over...** (Score:2)

by [Ironica \(124657\)](#) on Sunday December 14, @01:15PM (#7718052)  
(Last Journal: [Monday November 10, @03:50PM](#))

*If anything, this article sounds like a bunch of reporters got pissed, because they weren't allowed into a closed door conference, and broke the rules to get an access badge*

The original press release reported on /. ([here](#) [slashdot.org]) didn't mention that group of reporters at all, and this article doesn't actually discuss any link between the researchers and the reporters. I get the impression that the *Washington Times* thought the discussion of the pirate radio broadcast gave the story a little more color for those who find RFID boring.

Besides, would you feel just as fine about your security card at work if it flashed your personal details on a screen that can be read from 10 feet away, along with a queue of the last several people who walked in via that entrance? Is it enough for your boss to know that you just got back from lunch late, or should he know that you were at lunch with the same group of drinking buddies you always go with too?

**Ultimate Police State via RFID** (Score:1)

by [instarx \(615765\)](#) on Monday December 15, @01:07AM (#7722603)

The threat to privacy and democracy by RFID is NOT overblown. It seems clear to me that the wide acceptance of RFID tags is a serious threat to privacy and even to the democratic form of government. Here is an interesting scenario:

You walk down a street and a government scanner in a van detects that you went into a gun shop (or an opposition political party office or Greenpeace or an abortion-rights office or right-to-life office... you take your pick). That scanner is connected to a national Homeland Security database (probably named something like "Patriot Scanning and Verification System") that identifies you and simultaneously associates all your RFID tags. From that point on anytime you go anywhere those RFID detectors around town know exactly who and where you are. Because all those tags embedded in your clothes have now been associated with your RFID-embedded credit card they don't even have to have personal information on them to identify you. The government can now tell who you hang out with (aka "known associates") by associating your companions' tags with yours. They also know what cities you visit and where you go while you are there.

It won't even be possible to remove or smash all your tags to escape the spying. Just the act of having NO tags would raise a flag and single you out.

Do you think it unlikely that the government won't have agents walking around with RFID loggers at unpopular (to them) political rallies identifying all the subversives?

Simply by entering your name in their computer the government will be able to tell where you have gone, what political rallies you have attended, what activist organizations you have visited, where you travelled, what you bought, who your associates are, and even when you didn't leave your house for a week (no hits). **And they will be able to do this for every single person in the country!**

Is it really not a concern to you that this can easily be done today? Right now the only thing keeping the ultimate police state from being available to any paranoid right-wing administration, agency or government is that we simply aren't carrying around many of these RFID tags yet.

**Self-Defense** (Score:5, Insightful)

by [Quantum-Sci \(732727\)](#) on Sunday December 14, @12:13PM (#7717510)  
(<http://quantum-sci.com/>)

For those who doubt the concerns about RFID, it's about who controls your own information: you... or others.

We will get no regulation of the uses RFID is put to, while the Party is in power, and so it's up to us to sort this out.

Be advised that cellphone mfgs are now adding technology that PUSHes ads to you. Will you be able to turn it off? Doubtful; if all the carriers do it, there's no place else to go.

And of course CDMA has always had geo-location... they promise it's only used to catch indicted criminals, but that claim is very doubtful, given some recent events.

Delegates at a conference could be identified as they approach their car. Obscuring codes don't matter; a sample could be taken at any time prior, at great distance with a parabolic dish. Soldiers could be accurately geo-located by the enemy.

Did you know that all GM cars since 1999 have black boxes in them, which are NOT being used to help you understand what happened 5 seconds before an accident, but to INDICT you for that accident, and expose you to civil litigation as well. Your inanimate \*car\* has become a prosecution witness against you, even though your own wife isn't supposed to be forced to testify against you.

This is the difference between the old way, and the neo-way, of managing the citizens. The deeper question is, why is our society becoming more and more adversarial, so fast? How do Nordic countries and Canada, get away with cooperation, rather than ever strengthening offense and defense, every day? They don't worry about NOT being something, like we Americans do. Double-plus ungood.

You say that when out in public, you have no expectation of privacy? True, but RFID expands that 'public' from your immediate surroundings (which *you* are aware of, and choose to inhabit), to the known universe, and *for all time*. If in 10 years it is considered treasonous to question RFID, some of us will be screwed, now, won't we? We all go places we'd like to keep private sometimes, now, don't we? Care to give that up, for no good reason other than **FEAR?!** Of our own government/corporate oligopoly? How much of your day do you spend in **FEAR?!** WTF are you afraid of NOW, FGS?!

RFID is a great idea for inventory, but should be disabled/disablable when purchased. I doubt those chips now in tires, can be disabled, given the vulcanization process. And tags will soon be microscopic.

RFID has **no business** on a person, as long as corporations and politicians behave adversarially toward their public at the highest levels.

#### **RFID on slashdot stories** (Score:2, Funny)

by [Woy \(606550\)](#) on Sunday December 14, @12:19PM ([#7717558](#))

Maybe slashdot should add RFID to the stories, so that when they come the 2nd time around we can detect them right away...

#### **that's a lot of countries for so few people** (Score:2, Funny)

by [Engush \(732751\)](#) on Sunday December 14, @12:52PM ([#7717843](#))

*"The badges were handed out to more than 50 prime ministers, presidents and other high-level officials from 174 countries, including the United States."*

so each official was from an average of 3.5 countries?

#### **RFID is nothing new** (Score:3, Informative)

by [dacarr \(562277\)](#) <[ke6isf.spamcop@net](mailto:ke6isf.spamcop@net)> on Sunday December 14, @01:03PM ([#7717944](#))

(<http://www.northarc.com/~ke6isf> | Last Journal: [Saturday September 27, @02:32AM](#))

They use it to track runners for the LA Marathon. No biggie.

#### **So secretly, it was in the Times** (Score:1)

by Anonymous Coward on Sunday December 14, @01:13PM ([#7718028](#))

Now that's secrecy for you.

#### **Wow talk about security risk.** (Score:1)

by [DarkOx \(621550\)](#) on Sunday December 14, @03:42PM ([#7719201](#))

(<http://homepages.bw.edu/~gwalton>)

Imagine if the RFID numbers got leaked to the wrong people. An assassin could have the exact location of their target at all times. The consequence of such immoral behavior as undisclosed RFID tags could have been disastrous. Seeing as how nobody got hurt though this is probably a good thing. This happened to a lot of high level people with power to do something about this privacy threat as opposed to having happened to the rest of us where we would just be ignored. This is the type of thing that could really put the fear of God into these people too as far as the entire technology.

Imagine I want to knock someone off. I bribe the store clerk at a place he frequents to leave the tag on something he buys turn off the alarm and phone me the item number. He now has a nice homeing device that I can use to track him all around town and strike at the first good opportunity, fumbling with the keys to his apartment garage or something when no one is around. Not only are there privacy risks when important people are being tagged it could easily prove dangerous, that was just one potential situation.

**Re:Wow talk about security risk.** (Score:2)

by [black mariah \(654971\)](#) on Sunday December 14, @06:50PM (#7720572)

(Last Journal: [Saturday December 13, @03:22AM](#))

Or you could just follow him. Any more borderline paranoid notions you want me to shoot down?

**Re:Wow talk about security risk.** (Score:2)

by [Fuzzums \(250400\)](#) on Sunday December 14, @07:46PM (#7720886)

(<http://www.fuzzums.nl/> | Last Journal: [Sunday October 20, @08:24AM](#))

LOL: World peace is at stake here!

**It's all about marketing** (Score:2, Insightful)

by [UltraSkuzzi \(682384\)](#) on Sunday December 14, @04:20PM (#7719524)

(<http://www.werewolfsmg.net/>)

It didn't take long for that technology to be misused now did it? I can see the day when you go by RFID ready ad displays in the mall, and will be tailored to your 'interests' as they carefully read what stores you've been to and feed a 'relevant ad'. Pretty soon RFID TVs will be made too, all sorts of fun and interesting uses for this technology will pop up! yay! Take me now Lord.....

**Re:It's all about marketing** (Score:1)

by [p00ya \(579445\)](#) on Sunday December 14, @09:54PM (#7721654)

I can see the day when you go by RFID ready ad displays in the mall, and will be tailored to your 'interests' as they carefully read what stores you've been to and feed a 'relevant ad'.

Because none of us would actually want to see advertising material that's actually *relevant* to us now would we? This might be embarrassing in the middle of a mall, but FFS should we erase sales assistants' memories of your face so that they don't remember you the next time you come in to their store?

**Re:It's all about marketing** (Score:1)

by [Wyzard \(110714\)](#) on Sunday December 14, @10:47PM (#7721925)

(<http://www.lehigh.edu/~mbp2/>)

Reminds me of the newspapers and shopping-mall advertising seen in Minority Report...

**No expectation of privacy.** (Score:1)

by [mightyJohn \(129821\)](#) on Sunday December 14, @07:48PM (#7720900)

The system used by the conference identified badge holders at the door. Were attendees to think the badge magically communicated with security?

All the information that could be gathered by this RFID system is public- the system can only record when a tag moves within a proximity of a reader. Given the limited read distance of contemporary readers, this information could more effectively be gathered by hiring people to write down the names of attendees as they enter a room.

RFID is an extremely useful technology in broad use today. Imagine the backlash when the public finds out millions of automobiles are "bugged" with RFID tags (the E-Z Pass system.) This article irresponsibly suggests that RFID inherently threatens privacy.

More at RFID News, <http://www.rfidnews.org>

**Re:No expectation of privacy.** (Score:1)by [jifl \(471653\)](#) on Sunday December 14, @09:21PM (#7721468)

- > *All the information that could be gathered by this RFID system is*
- > *public- the system can only record when a tag moves within a proximity*
- > *of a reader. Given the limited read distance of contemporary readers,*
- > *this information could more effectively be gathered by hiring people*
- > *to write down the names of attendees as they enter a room.*
- > [snip]*This article irresponsibly suggests that RFID inherently threatens privacy.*

With **contemporary** readers, yes. With the way they seem to be taking off, how long will that last?

It would be like saying 15 years ago that mobile phones could never be the size they are today because the aerials and batteries would make them too big. Or that [factoring RSA-576](#) [slashdot.org] would be infeasible in the near future.

Technology advancement often has a way of exceeding your expectations, and exceeding your fears.

**Re:No expectation of privacy.** (Score:1)by [GnarlyNome \(660878\)](#) on Tuesday December 16, @01:27AM (#7732389)(Last Journal: [Sunday July 06, @09:18PM](#))

Divorce lawyers are already subpoenaing the Fastrac records of people involved in divorce cases

**Overblown as usual** (Score:2)by [John Harrison \(223649\)](#) on Sunday December 14, @08:49PM (#7721272)<http://www.angelfire...nirak/tutorial/day6/> | Last Journal: [Monday August 18, @05:45PM](#))

Slashdot (and now The Washington Times) seems unable to do an RFID story without a strong sense of panick. While this story has even less detail than the one posted a few days ago, it is pretty clear that nobody was being "secretly tracked". People attending the event presented their badges to enter a meeting and that event was logged. It isn't like they can tell where you are within a meter at any time. It also isn't entirely clear that these are RFID badges.

**In other news....** (Score:3, Funny)by [KC7GR \(473279\)](#) on Monday December 15, @01:08AM (#7722604)<http://www.bluefeathertech.com/> | Last Journal: [Thursday October 02, @01:31PM](#))

AP SPOOFWIRE -- Two microwave ovens were seriously damaged today at the Internet and Technology Conference in Switzerland when numerous conference attendees, annoyed when they discovered that their badges contained RFID chips, tried to disable those same chips through "nuking" them in the ovens.

Cafeteria staff were stunned by the spectacle produced when each oven was crammed full of badges, and the 'Start' button pressed. "I'd always heard stories about what would happen if you put anything with metal in it into a microwave" said head cook Rowena Splatt, "But I never thought I would ever see it in action! That horrible buzzing noise, the showers of sparks -- though I will admit that all those colors were kind of pretty -- but the smell! Oh, that was the worst part!! It reminded us all of last week's liver-and-onion special, with hints of burned cranberries and overcooked zucchini..."

Security personnel monitoring the RFID receiver systems also reported strange occurrences. "It was like thousands of these tinny little Munchkin-like voices screamed 'Help Meeeeeee!' all at once" reported Lt. Take-Emin Andbookem, head of security for the event. "And you wouldn't believe the volume! I've still got six people in the hospital, getting checked for hearing damage."

The event's organizers have reported that the badges will be reissued -- without RFID chips, this time -- and that the homogenized melted-together masses of the other badges will be made into holiday mobiles which will also feature unused AOL 9.0 CDs and old 30-pin memory SIMMs.

**Secret Service must be having a cow** (Score:1)by [Wardish \(699865\)](#) <[wardg.writeme@com](mailto:wardg.writeme@com)> on Monday December 15, @11:15AM (#7725140)(Last Journal: [Wednesday September 17, @03:35PM](#))

Imagine finding out after the fact that your charge "POTUS" was being electronically tracked through a structure with such bad security that a name and a 2 min fake id can overcome.

I would really hate to be the fellow in charge of that detail. His ulcers are probably having ulcers...

**UN's ITU wants to take over internet from ICANN??** (Score:2)

by [SkewlD00d \(314017\)](#) on Monday December 15, @01:24PM (#7726551)

(<http://www.slashduh.org/>)

I double-dog, thirty resolution dare them. Bring it; maybe they'll send in UN troops from Zimbabwe to Marina del Rey, CA (33.9803N, 118.4405W). Or maybe they'll RBL everything .us/.com/.net/.org/.gov to europe.... oh wait, that's 99% of the net; passive-aggressive seems to be the French way. Or, bring UNSECO in on it, let them make dozens of toothless resolutions: "The UN has become a point-less debating society" that panders to the little Fidel's of the world, along with the finger-pointing and empty threats to the Saddam's. Face it... ICANN (unfortunately, that dirty NGO) rules the net with a copper wire. Cut the cord, and there will be fighting over IPv4 subnet ownership and we'll end up w/ a fragmented internet (pun not intended). Let's just go to IPv6 (and not hand it over completely to big companies), and have a completely free TLD for dynamic dns / hobby kinda stuff, say .alt or something. Let's not give ownership to these dimwit politicians because they ask for it, and let's not allow big companies to create artificially low supply as the case is w/ IPv4 subnets. Stanford, UCB, UCD, etc. dont need a class B, it's completely stupid how every admin and bozo employee has a public, unfirewalled IP.

**Re:HEY, AMERICA!** (Score:1)

by [Quantum-Sci \(732727\)](#) on Sunday December 14, @04:39PM (#7719685)

(<http://quantum-sci.com/>)

Did you know that one of our Generals recently, *actually said* that if there is a national emergency, the first American dictator would have to be appointed?

WTF?! Are we being prepared?

How bad of an emergency? Like 9/11? And exactly who decides? Dick Cheney, as usual?!?!?

**Re:HEY, AMERICA!** (Score:1)

by [kommakazi \(610098\)](#) on Sunday December 14, @04:44PM (#7719714)

I wasn't kidding, actually...

That is when the public revolts.

**Re:HEY, AMERICA!** (Score:1)

by [Quantum-Sci \(732727\)](#) on Sunday December 14, @04:49PM (#7719750)

(<http://quantum-sci.com/>)

Actually, that's when intellectuals depart from the masses, but have little effect.

The masses will put up with anything, witness Soviet Russia and N. Korea.

**Re:HEY, AMERICA!** (Score:2, Interesting)

by [kommakazi \(610098\)](#) on Sunday December 14, @04:55PM (#7719805)

And the USA/world? post GWB.

I want to leave the country for exactly that reason.

**Re:HEY, AMERICA!** (Score:1)

by [kaatochacha \(651922\)](#) on Tuesday December 16, @07:04PM (#7740669)

If I remember correctly, it was Tommy Franks who said it, and he was warning about losing our consitution if a WMD even led us silly people to abandon the constitution for security. not advocating, but warning against.

**Re:HEY, AMERICA!** (Score:1)

by [kommakazi \(610098\)](#) on Sunday December 14, @10:47PM (#7721927)

My question is, how is this "Flamebait"?

Going by GWB's track record so far, would this really be all that suprising? And really I saw no flame war started after I posted this....

**yeh and CNN** (Score:1)

by [GnarlyNome \(660878\)](#) on Tuesday December 16, @01:31AM (#7732409)

(Last Journal: [Sunday July 06, @09:18PM](#))

Was founded by Ted "Better Red Than Dead " Turner

[Site Map](#)
[Front Page](#)
[Nation/Politics](#)
[-Pruden on Politics](#)
[-Inside the Beltway](#)
[-Inside Politics](#)
[-Inside the Ring](#)
[-Federal Report](#)
[-Around the Nation](#)
[-Daybook](#)
[-Steiner Cartoon](#)
[World](#)
[Commentary](#)
[Editorials/Op-Ed](#)
[Metropolitan](#)
[Sports](#)
[Business](#)
[Special Reports](#)
[Technology](#)
[Entertainment](#)
[Books](#)
[Food](#)
[Wash. Weekend](#)
[Travel](#)
[Family Times](#)
[Culture, etc.](#)
[Civil War](#)
[Weather](#)
[Corrections](#)
[Classifieds](#)
[Home Guide](#)
[Auto Weekend](#)
[Employment](#)
[Health](#)
[Services Directory](#)
[Market Place](#)
**Special Offer...**

## Health Insurance You CAN Afford!!

[Don't Gamble With Your Family's Health! click here for more information](#)

December 14, 2003


[Advertising](#)

## Bug devices track officials at summit

By Audrey Hudson

THE WASHINGTON TIMES

Officials who attended a world Internet and technology summit in Switzerland last week were unknowingly bugged, said researchers who attended the forum.

Badges assigned to attendees of the World Summit on the Information Society were affixed with radio-frequency identification chips (RFIDs), said Alberto Escudero-Pascual, Stephane Koch and George Danezis in a report issued after the conference ended Friday in Geneva. The badges were handed out to more than 50 prime ministers, presidents and other high-level officials from 174 countries, including the United States.

The trio's report said they were able to obtain the official badges with fraudulent identification only to be stunned when they found RFID chips — a contentious issue among privacy advocates in the United States and Europe — embedded in the tags.

Researchers questioned summit officials about the use of the chips and how long information would be stored but were not given answers.

The three-day WSIS forum focused on Internet governance and access, security, intellectual-property rights and privacy. The United States and other countries defeated an attempt to place the Internet under supervision of the United Nations.

RFID chips track a person's movement in "real time." U.S. groups have called for a voluntary moratorium on using the chips in consumer items until the technology and its effects on privacy and civil liberties are addressed.

Mr. Escudero-Pascual is a researcher in computer security and privacy at the Royal Institute of Technology in Stockholm. Miss Koch is the president of Internet Society Geneva, and Mr. Danezis studies privacy-enhancing

### TOP STORIES

- Dean's candidacy inspires shock, awe
- Bug devices track officials at summit
- Officials fearful flu could develop into a pandemic
- President Bush addresses nation
- Land available for Flight 93 memorial
- D.C. nonbinding primary may have clout
- Blood banks suffer shortage

### BREAKING NEWS

#### FROM AP

- Captured Saddam Faces Tough Interrogation
- Chamber Beneath Mud Hut Leads to Hussein
- Iraqis Surprised Saddam Didn't Fight
- N. Korea Rejects U.S. Nuke Crisis Remedy
- Palestinian-Canadian Charged in Israel
- U.S. Officials to Meet Mideast Leaders
- Car Bomb at Iraqi Police Station Kills 17
- Saddam's Capture May Aid Bin Laden Search
- Turkish Cypriot Elections End in Deadlock
- Assassination Attempt on Musharraf Fails

#### FROM UPI

- 'Ladies and gentlemen: we got him!'
- UPI NewsTrack TopNews
- Peru bus crash kills 24 people
- Poll: Americans' support for Iraq war up
- Two police officers shot to death
- Eye for an eye in Pakistan courtroom
- U.S. officials seek flu vaccine from U.K.
- Chinese trial begins for September orgy

Stay informed -  
get the  
right books

Take **5** books for  
**\$1**  
Plus a **FREE Gift!**

[Click for details](#)


### FEATURE MARKETPLACE

[For The Home](#)
[Electronics / Computers](#)
[Education](#)
[Health](#)
[Entertainment](#)
**NEW!!!**
[Grocery Coupons](#)



[Tourist Guide](#)[Holiday Gift Guide](#)[International Reports](#)[Archive](#)[Subscription](#)[Advertise](#)[About TWT](#)[Contact Us](#)[TWT Gift Shop](#)[Insight Magazine](#)[The World & I](#)[National Weekly](#)[Middle East Times](#)[Tiempos del Mundo](#)[Segye Ilbo](#)[Segye Times USA](#)[Chongyohak Shinmun](#)[Sekai Nippo](#)[Wash. Golf Monthly](#)

technologies and computer security at Cambridge University.

"During the course of our investigation, we were able to register for the summit and obtain an official pass by just showing a fake plastic identity card and being photographed via a Web cam with no other document or registration number required to obtain the pass," the researchers said.

The researchers chose names for the fake identification cards from a list printed on the summit's Web site of attendees.

The hidden chips communicate information via radio frequency when close to sensors that can be placed anywhere "from vending machines to the entrance of a specific meeting room, allowing the remote identification and tracking of participants, or groups of participants, attending the event," the report said.

The photograph of the person and other personal details are not stored on the chip but in a centralized database that monitors the movement. Researchers said they are concerned that database will be used for future events, including the next summit to be hosted by Tunisian authorities.

"During the registration process, we requested information about the future use of the picture and other information that was taken, and the built-in functionalities of the seemingly innocent plastic badge. No public information or privacy policy was available upon our demands that could indicate the purpose, processing or retention periods for the data collected. The registration personnel were obviously not properly informed and trained," the report said.

The lack of security procedures violates the Swiss Federal Law on Data Protection of June 1992, the European Union Data Protection Directive, and United Nations' guidelines concerning computerized personal-data files adopted by the General Assembly in 1990, the researchers said.

"The big problem is that system also fails to guarantee the promised high levels of security while introducing the possibility of constant surveillance of the representatives of civil society, many of whom are critical of certain governments and regimes," the report said.

"Sharing this data with any third party would be putting civil-society participants at risk, but this threat is made concrete in the context of WSIS by considering the potential impact of sharing the data collected with the Tunisian government in charge of organizing the event in 2005," it said.

The organization Reporters Without Borders was banned from attending the summit and launched a pirate radio broadcast to protest the ban and detail press-freedom violations by some countries attending the meetings, including Tunisia.

"Our organization defends freedom of expression on the Internet on a daily basis. Our voice should therefore be heard during this event, despite this outrageous ban," said Robert Menard, secretary general of Reporters Without Borders.

Tunisia is among several countries Reporters Without Borders has accused of censoring the Internet, intercepting e-mails and jailing cyber-dissidents.

[Print this article](#)[Back to Nation/Politics](#)[E-Mail this article](#)

£69.00  
per year  
incl VAT

ISP directory  
Features

News

Support

⌘ Email story to a friend

⌘ Print this news article

⌘ Submit your story

⌘ Add comments

⌘ Margaret Dennis

ISP  
**NEWS**

## ▲ Officials bugged at international summit

Sunday 14 December 2003, 19:27:08

 All Countries

Written by **Margaret Dennis**

The World Summit on the Information Society held in Geneva ended last Friday. Researchers attending the conference have exposed the use of radio-frequency identification chips (RFIDs) found embedded in identification tags used for the summit.

Prime ministers and presidents were among the attendees from 174 countries who were allegedly bugged.

The information was released by three researchers who fraudulently obtained the official badges and were shocked to discover the bugs imbedded the tags.

The main focus of the three day summit was internet governance, access, security, intellectual property rights and privacy.

At the summit, a plan to place the internet under the supervision of the United Nations was defeated.

The researchers who made the discovery of the RFIDs were Mr Escudero-Pascual, a researcher in computer security and privacy at the Royal Institute of Technology in Stockholm, Miss Koch, president of Internet Society Geneva, and Mr Danezis who studies privacy-enhancing technologies and computer security at Cambridge University.









*"During the course of our investigation, we were able to register for the summit and obtain an official pass by just showing a fake plastic identity card and being photographed via a Web cam with no other document or registration number required to obtain the pass," the researchers said.*

*RFIDs transmit information to sensors that may be placed anywhere "from vending machines to the entrance of a specific meeting room, allowing the remote identification and tracking of participants, or groups of participants, attending the event," the report said.*




*The trio approached officials about the RFIDs asking how long the gathered information would be stored but were not given an answer. Their fear is that the information will be used for other events such as the next summit due to be hosted by Tunisia.*



### Other News

-  Surf 24-7 drops standard broadband prices
-  Does Big Blue have the cheapest Internet Access?
-  BT announces new services
-  Tiscali announces PAYG broadband
-  BT goes underwater
-  Partnership will save your telephone bill
-  Tiscali broadband product ascends market
-  Broadband for under \$50

### More On Internet - General

-  EBay launches \$50,000 SOHO competition
-  A Generation of Internet Savvy Users
-  Google still number 1

"During the registration process, we requested information about the future use of the picture and other information that was taken and the built-in functionalities of the seemingly innocent plastic badge. No public information or privacy policy was available upon our demands that could indicate the purpose, processing or retention periods for the data collected. The registration personnel were obviously not properly informed and trained," the report said.

The use of the RFIDs was in violation of several laws: the Swiss Federal Law on Data Protection of June 1992, the European Union Data Protection Directive, and United Nations guidelines concerning computerized personal-data files adopted by the General Assembly in 1990.

"The big problem is that system also fails to guarantee the promised high levels of security while introducing the possibility of constant surveillance of the representatives of civil society, many of whom are critical of certain governments and regimes," the report said.

"Sharing this data with any third party would be putting civil-society participants at risk, but this threat is made concrete in the context of WSIS by considering the potential impact of sharing the data collected with the Tunisian government in charge of organizing the event in 2005," it said.

Source: The Washington Times

- :: [Email this story to a friend](#)
- :: [Print this news article](#)
- :: [Submit your story](#)

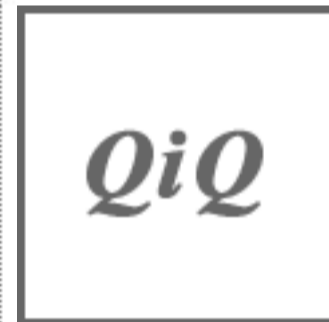
### ▲ News Comments

There are currently no comments for this news article.

:: [Add comments](#)

**▲ Free newsletter**  
Subscribe to the Net4Nowt Newsletter!  
[Click here for details.](#)

**▲ Recommend this page**  
Recommend this page to a friend by  
[clicking here.](#)



**THEFEATURE** ::

IT'S ALL ABOUT THE MOBILE INTERNET

HOME

TOPICS

MOBILE

SIGNUP

SITE MAP

SEARCH

HELP

TheFeature: howard: Journal: Why did WSIS bug delegates?

**howard's Page****Howard Rheingold**Karma: **Excellent**

JOURNAL

howard's journal:

**Why did WSIS bug delegates?** Dec 15 2003 5 comments

I wonder whether we'll ever know why clandestine RFID tags were implanted in the ID badges of delegates to the World Summit on the Information Society. An independent group of activist researchers discovered that all of the identification badges issued to delegates contained RFID chips capable of tracking the wearers' location. Alberto Escudero-Pascual, Stephane Koch and George Danezis attended the event after presenting valid personal ID. In [this press release](#), the three computer professionals detailed their discovery of the RFIDs embedded in the Summit badges: *The official Summit badges, which are plastic and the size of a credit card, hide a "RF smart card" [1] - a hidden chip that can communicate its information via radio frequency. It carries both a unique identifier associated with the participant, and a radio frequency tag (RFID) that can be "read" when close to a sensor. These sensors can be located anywhere, from vending machines to the entrance of a specific meeting room allowing the remote identification and tracking of participants, or groups of participants, attending the event. The data relating to the card holder (personal details, access authorization, account information, photograph etc.) is not stored on the smart card itself, but instead managed by a centralized relational database. This solution enables the centralized system to monitor closely every movement of the participants at the entrance of the conference center, or using data mining techniques, the human interaction of the participants and their relationship. The system can potentially be extended to track participants' movements within the summit and detect their presence at particular session.*

**rfids do not equal bugs**

ericLin, Dec 15 2003

i understand your concern howard. really, of all places, you would think that at a conference like WSIS they would inform the delegates of the technology included in their badges and how it was being used. however the claim that the delegates were "bugged" or tracked is just a guess at one way in which the technology *could* be used. we have no way of knowing (at least not yet) whether it was actually used this way. sure, the hosts could easily track the exchange of the badge and any reader the delegates used it on, but that doesn't mean they tracked more than that. concern over this is not all that different from concern over cameraphones. just because they *can* be used for unsavory applications does not mean they are *only* used for unsavory applications. i also believe that keeping all the attendee data in a central database may have actually been safer than programming onto the card. it should make it more difficult for malicious people to get a hold of the data than if those bits were flowing all around the conference via rfid or smartcard readers. do we have any proof, or even any good suspicions that the attendees were really bugged?

**MEMBER LOGIN**

User name

Password

Remember me **SIGN UP****SEARCH THEFEATURE****EDITOR'S CHOICE**[3G: A Soft Launch Is Bett... \(+4\)](#)

By Steve Wallage, Mon Mar 01 12:15:00 GMT 2004

**MEMBER BENEFITS****TELEMATICS DETROIT 2004**

**re: rfids do not equal bugs**

howard, Dec 16 2003

A nearly invisible chip was put in their ID tags, a chip that knows who they are, and is capable of transmitting that information to a card reader, and the delegates weren't told about it. I'd say that no further conspiracy theory is necessary -- giving someone an ID badge with an RFID chip without informing them is a bad enough offense, even if there are no sinister uses planned for the information gathered. Why install such a chip if it isn't going to be used? If it's going to be used for something innocuous, shouldn't the badgeholders be told. I don't know the other authors, but I know that Alberto Escudero-Pascual is a serious student of the privacy impacts of communication media. He can't afford the damage to his academic reputation to come out with an accusation like this unless it's true and has serious implications.

**The problem: inadequate disclosure**

howard, Dec 16 2003

From the press release: *<i>* During the registration process we requested information about the future use of the picture and other information that was taken, and the built-in functionalities of the seemingly innocent plastic badge. No public information or privacy policy was available upon our demands, that could indicate the purpose, processing or retention periods for the data collected. The registration personnel were obviously not properly informed and trained. Our main concern is not only that the Summit participants lack information about the functionalities of this physical access system implemented, or that no one was able to answer questions of how the personal data would be treated after the Summit. The big problem is that system also fails to guarantee the promised high levels of security while introducing the possibility of constant surveillance of the representatives of civil society, many of whom are critical of certain governments and regimes. Sharing this data with any third party would be putting civil society participants at risk, but this threat is made concrete in the context of WSIS by considering the potential impact of sharing the data collected with the Tunisian government in charge of organizing the event in 2005.

**That is...**

howard, Dec 16

2003

Nobody is claiming that the RFIDs are microphones, in the classic sense of "bug," but they are certainly devices capable of recording aspects of the unsuspecting badgeholders' behavior, and in that sense they are, in my opinion, a bug -- in the sense of a clandestine device intended to capture information about individuals without their knowledge.

**engineers and their toys**

johnjc, Dec 16 2003

It looks to me like ITU engineers playing with their new toys. You have to admit it's a fun technology, and if they'd told people there would have been a stink - during the meeting. They might even have had their toys taken away from them. Seriously, I think it was just that, coupled with naivety that they thought they could get away with it. The naivety was there whatever the rest of the explanation. The two papers they approved which form the official results of the summit were worked out before the summit formally opened - that's how these meetings are meant to work and they had two extre preparatory meetings to get those documents approved. So it's hard to imagine what serious intent they might have had - unless you go really paranoid and figure "somebody" was just on a fishing expedition to see what he could learn about who people hung out with.

[Back to howard's Journal](#)



# WSIS, i delegati erano spiati

Press Releases on

**INTERNET**

08/03/2004 | [PRESS](#)

[CONFERENCE: "FOURTOU REPORT AND DIGITAL FREEDOM"](#)

08/03/2004 | [CONFERENZA](#)

[STAMPA: "RAPPORTO FOURTOU E LIBERTA' DIGITALI"](#)

18/02/2004 | [TUNISIA. CAPPATO:](#)

["95 DEPUTATI DI TUTTI I GRUPPI POLITICI CHIEDONO LIBERAZIONE CYBERDISSIDENTI IN VISTA DEL SUMMIT MONDIALE SULLA SOCIETA' DELL'INFORMAZIONE \(WSIS\)".](#)

18/02/2004 | [TUNISIA. CAPPATO:](#)

["95 MEPS OF ALL POLITICAL GROUPS CALL FOR THE LIBERATION OF THE CYBER-DISSIDENTS IN THE RUN-UP TO THE WORLD SUMMIT ON THE INFORMATION SOCIETY \(WSIS\)".](#)

18/02/2004 | [TUNISIE. CAPPATO:](#)

["95 DÉPUTÉS DE TOUS LES GROUPES POLITIQUES DEMANDENT LA LIBÉRATION DES CYBERDISSIDENTS EN VUE DU SOMMET MONDIAL SUR LA SOCIÉTÉ DE L'INFORMATION \(WSIS\)".](#)

17/02/2004 | [MARCO CAPPATO](#)

[ALLA CONFERENZA INTERNAZIONALE SUL FREE SOFTWARE CON L'EX-PRESIDENTE SPAGNOLO FELIPE GONZÁLEZ.](#)

17/02/2004 | [MARCO CAPPATO AT](#)

[THE MALAGA INTERNATIONAL FREE SOFTWARE CONFERENCE WITH SPANISH EX-PRESIDENT FELIPE GONZÁLEZ](#)

12/12/2003 | [ONU / SUMMIT SOC.](#)

[INFO: TUNISIA E CUBA CONTRO I RADICALI](#)

11/12/2003 | [ONU / SUMMIT SOC.](#)

[INFO: CAPPATO "NIENTE SOLDI AI DITTATORI DIGITALI"](#)

16/12/2003 | Punto Informatico | INTERNET |  

16/12/03 - News - Roma - Si parlava di comunicazione digitale, di sicurezza e riservatezza dei dati, di libera circolazione dei saperi e di avvento di internet a Ginevra la scorsa settimana e chi ne parlava non sapeva di essere tracciato. Gli spostamenti di migliaia di persone al World Summit on the Information Society (WSIS) sono stati seguiti da un occhio, anzi un chip, invisibile.

Ad accusare gli organizzatori svizzeri del WSIS di aver fatto ricorso a chip su radiofrequenza RFID senza neppure dirlo ai delegati sono tre ricercatori che alla fine del meeting internazionale hanno rilasciato un rapporto di denuncia sull'accaduto ripreso, tra gli altri, anche dal Washington Post.

Alberto Escudero-Pascual dell'Istituto reale di Tecnologia di Stoccolma, Stephane Koch, presidente della Internet Society di Ginevra e George Danezis, ricercatore di Cambridge sono tre personaggi super partes che non hanno affatto gradito la sorpresina preparata dal WSIS ai delegati. E hanno dimostrato che all'interno dei badge che venivano rilasciati per l'accesso alle aree del WSIS erano piazzati dei chip a radiofrequenza capaci, stando al rapporto, a seguire gli spostamenti dei singoli intervenuti nelle diverse aree della conferenza.

I chip RFID, dunque, sono stati piazzati non solo nei badge di giornalisti, segretari e attendenti vari ma anche in quelli di una 50ina di primi ministri, rappresentanti governativi e funzionari di alto livello, compresi anche molti rappresentanti italiani. A nessuno di loro, però, è stato detto alcunché sulla presenza degli RFID e lo stesso WSIS, hanno spiegato i tre ricercatori, non si è dotato di una policy sulla privacy pubblica né ha saputo spiegare questa particolarissima scelta. Basti pensare che anche in Svizzera, come fin qui

## Other articles on INTERNET

09/03/2004 | Punto Informatico

[Proprietà intellettuale, oggi l'Europa decide](#)

05/03/2004 | Punto Informatico

[Domini, Stanca difende l'ICANN](#)

21/01/2004 | Wired News

[Open-Source E-Voting Heads West](#)

08/01/2004 | GNU

[World Summit on the Information Society](#)

16/12/2003 | Punto Informatico

[WSIS, i delegati erano spiati](#)

15/12/2003 | www.epochtimes.com

[Article on the Conference organized by the Transnational Radical Party in Geneva "Democracy, Freedom and Digital Divide"](#)

14/12/2003 | THE WASHINGTON TIMES

[Bug devices track officials at summit](#)

14/12/2003 | The Boston Globe

[The Internet's role in media freedom](#)

12/12/2003 | Diario Nacional Granma-enlinea

[Ataque respondido](#)

12/12/2003 | Terra Viva

[Les Etats-voyous de l'information](#)

12/12/2003 | Il Foglio

[Dei diritti e di Internet. Note radicali per esportare la democrazia sulla Rete](#)

03/12/2003 | AlterNet

**>>>more Press Releases on  
INTERNET**

in Europa, l'adozione degli RFID viene valutata con molta attenzione nel timore che la loro introduzione nei prodotti di largo consumo possa tradursi in una violazione amplissima della privacy delle persone.

"Nel corso delle nostre indagini - ha spiegato Escudero-Pascual - siamo riusciti a registrarci per il Summit ed ottenere un pass ufficiale semplicemente mostrando una carta di identità fasulla e accettando di essere fotografati da una webcam, non abbiamo dovuto fornire altri documenti o numeri di registrazione per ottenere il pass". Secondo i tre ricercatori, i chip RFID potevano essere letti da qualsiasi cosa, come "i distributori automatici all'ingresso di una specifica sala riunioni, in modo da consentire l'identificazione dei partecipanti o di gruppi di partecipanti".

Il timore espresso nel rapporto è che le informazioni raccolte con gli RFID vengano poi utilizzate in ambito pubblico soprattutto in vista del secondo round del WSIS previsto a Tunisi per il 2005. "Abbiamo chiesto - hanno spiegato i tre - quale sarebbe stato l'uso dei dati da loro raccolti ma il personale addetto, ovviamente, non ne sapeva nulla". Secondo i tre scienziati il WSIS ha violato una serie di norme sulla riservatezza, in particolare la Legge sulla protezione dei dati personali approvata in Svizzera nel 1992, la Direttiva europea sulla privacy nonché le linee guida ONU sull'uso dei file personali del 1990.

"Il problema maggiore - hanno spiegato i tre ai reporter - è che questo sistema non offre adeguata sicurezza ma consente invece la sorveglianza costante dei rappresentanti della Società Civile, molti dei quali criticano certi regimi e certi governi. La condivisione di dati con una terza parte potrebbe mettere tutti loro a rischio e questa possibilità è ora concreta nell'ambito del WSIS se si considera l'impatto che potrebbe avere la condivisione dei dati con il governo tunisino che nel 2005 dovrà organizzare l'evento".

A non avere addosso il chip, paradossalmente, erano invece gli hacktivist che sono entrati al WSIS con badge fasulli per dimostrare l'inefficienza dell'apparato di sicurezza dell'evento.

**Bringing Down the House**

---

20/11/2003 | Punto Informatico

**Rilasciato cyber-dissidente  
tunisino**

---

14/11/2003 | ZDNet

**Le président tunisien Ben Ali  
décore le père de l'internet  
Vinton Cerf**

---

13/11/2003 | Punto Informatico

**Brevetti, rinvii in Europa ed  
urgenze**

---

**>>>more articles on  
INTERNET**

[Site Map](#)
[Front Page](#)
[Nation/Politics](#)
[-Pruden on Politics](#)
[-Inside the Beltway](#)
[-Inside Politics](#)
[-Inside the Ring](#)
[-Federal Report](#)
[-Around the Nation](#)
[-Daybook](#)
[-Steiner Cartoon](#)
[World](#)
[Commentary](#)
[Editorials/Op-Ed](#)
[Metropolitan](#)
[Sports](#)
[Business](#)
[Special Reports](#)
[Technology](#)
[Entertainment](#)
[Books](#)
[Food](#)
[Wash. Weekend](#)
[Travel](#)
[Family Times](#)
[Culture, etc.](#)
[Civil War](#)
[Weather](#)
[Corrections](#)
[Classifieds](#)
[Home Guide](#)
[Auto Weekend](#)
[Employment](#)
[Health](#)
[Services Directory](#)
[Market Place](#)


## BMW X3

reviewed by AutoWeekend  
[click here to read](#)

December 18, 2003



Advertising ▼

## Summit group confirms use of ID chip

By Audrey Hudson and Betsy Pisik  
 THE WASHINGTON TIMES

Organizers of the World Summit on the Information Society yesterday confirmed that badges worn by high-level attendees were affixed with identification chips some say were unknown to the forum's participants.

However, a spokesman for the International Telecommunication Union (ITU), which was the host of the three-day event in Geneva last week, scoffed at concerns by privacy advocates that the technology could monitor an individual's movement or that the data it collects could be misused.

Three European researchers who discovered the chips in their badges, first reported by The Washington Times on Sunday, said participants were not told about the chips.

ITU spokesman Gary Fowlie confirmed during an interview from Geneva that radio frequency identification chips (RFIDs) were embedded in the passes and that data readers were in place to record information transmitted by the chip.

Mr. Fowlie disputed that RFIDs have long-range tracking capability, and called The Times story "really off base."

"Transmission distance is 1 to 2 centimeters. You have to put your badge right up to the screen," he said.

But U.S. and European privacy advocates and critics of RFID technology said the story was on target, and that the use of the chips at the summit has caused an uproar in the United States and Europe.

"It sent off a shot heard round the world," said Katherine Albrecht, director of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), a leading opponent of RFID technology.

"We're rolling in e-mails on this thing. It's confirmation this is real, it is here, and it's being abused already."

Last week's summit, which was partly organized by the United Nations,

### TOP STORIES

- Albright's joke joins growing list of Bush theories
- Bush marriage stance not 'clear'
- Summit group confirms use of ID chip
- Groups sue over immigration data
- Hinckley freed for day trips

### BREAKING NEWS

#### FROM AP

- Sharon: Israel May Move Some Settlements
- Rebels Kill One U.S. Soldier in Iraq
- Royal Coroner to Hold Princess Di Inquest
- Niagara Falls Survivor Fined for Stunt
- French Muslim Girls Eye Catholic Schools
- Clark: Milosevic Warned of Massacre
- Taiwan SARS Case Doesn't Worry Officials
- Russian President to Seek Second Term
- Canada Promises to Revive Pot Bill
- Ireland Will Probe 1989 IRA Killings

#### FROM UPI

- U.S. natural gas draws still above average
- Arnold orders funds for California cities
- Michael Jackson charged with molestation
- No one injured in FedEx plane fire
- Jury: Malvo guilty on all charges
- Plotters behind Zambia coup set to hang
- Refugees in Kenya face food shortage
- Tapes show abuse of immigrant detainees

Stay informed -  
 get the right books

Take **5** books for **\$1**  
 Plus a FREE Gift!

[Click for details](#)



### FEATURE MARKETPLACE

[For The Home](#)
[Electronics / Computers](#)
[Education](#)
[Health](#)
[Entertainment](#)
**NEW!!!**
[Grocery Coupons](#)



[Tourist Guide](#)[Holiday Gift Guide](#)[International Reports](#)[Archive](#)[Subscription](#)[Advertise](#)[About TWT](#)[Contact Us](#)[TWT Gift Shop](#)[Insight Magazine](#)[The World & I](#)[National Weekly](#)[Middle East Times](#)[Tiempos del Mundo](#)[Segye Ilbo](#)[Segye Times USA](#)[Chongyohak Shinmun](#)[Sekai Nippo](#)[Wash. Golf Monthly](#)

focused on Internet governance and access, security, intellectual-property rights and privacy. The badges were worn by more than 50 prime ministers, presidents and other high-level officials from 174 countries, including a representative from the United States, John Marburger, head of the White House Office of Science and Technology Policy.

In a lengthy statement to The Times yesterday, summit officials said participants were notified some personal information would appear on the Internet, but declined to say whether participants were told of the embedded technology.

The passes were intended "to facilitate identification by security at entry checkpoints," and participants had to swipe the badges across the readers to gain access to the summit and meeting rooms, the statement said.

"Readers were quite prominently displayed and were only placed at entry checkpoints," WSIS spokeswoman Francine Lambert said. "The data stored on our servers do not and cannot monitor movement."

U.S. companies use RFID chips to track inventory from the factory to stores. Manufacturers also are testing a system that tracks products leaving the shelves and alerts employees to restock.

EZ Pass, used at toll booths, uses RFID technology. Authorities investigating the murder of federal prosecutor Jonathan P. Luna learned that he had made repeated trips to Philadelphia during the past six months by tracking electronic data gathered at toll booths in Pennsylvania and Delaware.

The Defense Department is requiring its top 100 suppliers to implement RFID technology by 2005 to track inventory. The remainder of its 43,000 suppliers must ship items RFID-ready by 2006.

But privacy advocates say the technology Mr. Fowlie described in use at the summit can be used on humans.

"It's going to be used to track us," said Barry Steinhardt, director of the technology and liberty program for the American Civil Liberties Union in New York.

The ACLU said it has received complaints from Europeans concerned about how data collected at the summit will be used at the 2005 summit, where Tunisia plays host.

"There is a lot of concern this data will be transferred to Tunisia and used to punish citizens or residents, or to keep tabs on the participants who are coming there, perhaps deny entry," Mr. Steinhardt said. "There is a lot of concern that this data will be transferred to a less-than-democratic nation."

Ms. Lambert said the data was stored for one day on the readers and erased, but did not say how long data was stored on the database or if it was ever erased.

"The actual data submitted by participants was stored on ITU-secured servers that were not accessible by any other party than the [ITU, United Nations, and WSIS executive secretariat], and the data has not been communicated to any other party," she said.

The personal data was obtained from visa applications.

"This has tremendous value for intelligence gathering," said Alberto Escudero-Pascual, a researcher in computer security and privacy at the Royal Institute of Technology in Stockholm.

The chips were discovered by Mr. Escudero-Pascual, Stephane Koch, president of Internet Society Geneva, and George Danezis, a researcher of privacy-enhancing technologies and computer security at Cambridge University.

When the card containing an RFID chip is swiped onto the reader, the location information is sent via the chip's antenna to a database that contains information on the subject.

Mr. Escudero-Pascual said he witnessed the data collected by the summit when his information flashed on a computer screen at an entry point. The information included a picture of the participant, name, occupation, organization, a time stamp of all main entry points and each time the participant passed a line into a room.

# Nation/Politics

o has Alberto been queuing with for the

usually see who Alberto is working with or talking to by who he enters with," Mr. Escudero-Pascual said.

"This is not a conspiracy theory. We use these systems in our daily lives to open garages, but people are not aware" of other ways the technology can be used, he said.

RFID chips are embedded in many "smart card" systems used for access to military bases, airports, gated communities, hospitals, state parks and country clubs. RFID chips also can alert government agencies to a host of law-breaking activities, such as expired insurance policies or license plates.

But tagging participants in a political summit raises privacy and security issues, and privacy advocates think the summit's organizers might have broken laws by not disclosing the chips' presence.

At least one of the researchers said it violates the Swiss Federal Law on Data Protection of June 1992.

"They may be exempt from those laws, but they certainly violated the spirit of the law by collecting highly personal information without their knowledge or consent," Mr. Steinhardt said.



Print this article

[Back to Nation/Politics](#)



E-Mail this article



► ZDNET

► ACTUALITÉS

► TECH UPDATE

► BUILDER

► PRODUITS

► TÉLÉCHARGER

► SHOPPING

Accueil | Business | Technologie | Internet | Vidéos | Opinions | Archives

Rechercher sur ZDNet...

Recherche rapide:

 Antivirus
  Portables
  Ecran plat

Actualités &gt; Technologie

## RFID: les badges du sommet de Genève avaient des effets seconds

Par Christine TréguierZDNet France  
Mardi 23 décembre 2003



Réagissez à cet article.

**Le sommet mondial de la société de l'information, organisé à la mi-décembre à Genève par l'Union internationale des télécoms, a caché un détail important à ses participants. Leur badge contenait une puce électronique ou RFID, outil de traçage potentiel.**

Des puces RFID (Radio Frequency Identification) permettant de tracer le déplacement des objets ou des personnes étaient intégrées dans les badges des participants au Sommet mondial de la société de l'information (SMSI). Tous les participants (presse, société civile, industriels comme délégués officiels), et sans qu'ils en soient correctement avertis, ont reçu ces badges "sans contact" comme sésame pendant les trois jours du sommet.

L'information a été [dévoilée le 10 décembre](#) par trois universitaires et experts européens en sécurité informatique, qui ont étudié leurs propres badges. Ils ont la forme d'une carte de crédit, portant le nom du participant et une photo numérisée, prise sur place. Selon Stéphane Koch, consultant en cybercriminalité et, par ailleurs, président du chapitre suisse de l'Internet Society de Genève, le haut niveau de sécurité d'accès n'était pas garanti comme promis: on pouvait facilement s'inscrire sous une fausse identité et les photos, ne portant pas de marquage par hologramme, étaient facilement interchangeables. Ces puces ont été fabriquées par Sport Access, filiale de Kudelski, la société qui produit notamment les décodeurs de Canal Plus.

### La loi suisse imposait à l'UIT d'informer les participants

▼ publicité

Rappelons brièvement que ces puces radio (surnommées par leurs détracteurs des "PeRFIDes") contiennent chacune un numéro identifiant unique, radiotransmis automatiquement à tout lecteur situé dans un rayon de 2 centimètres à 2 mètres.

Mais il y a plus grave, poursuit Stéphane Koch: l'Union internationale des télécoms (UIT – l'organisateur du SMSI), «aurait du avertir les participants qu'ils se baladaient avec une puce moucharde autour du cou». D'autant qu'en Suisse, la loi sur la protection des données lui imposait cette démarche.

Gary Fowlie, directeur du service communication de l'UIT à Genève, réagit pour *ZDNet* à ces accusations: «Les lecteurs étaient très en vue et [placés] uniquement aux points d'entrée, comme à celui de la zone VIP» dit-il. Le rayon d'action des lecteurs «était limité à 2 centimètres», ce qui suppose en effet que le participant devait s'approcher près du lecteur pour entrer, évitant ainsi d'être "scanné" à son insu. Fowlie assure enfin: «Il n'y a pas eu de tracking des participants.»

### Les données des lecteurs effacées chaque soir

Alberto Escudero-Pascual, chercheur en sécurité à l'Institut royal de Stockholm, est sceptique:

### Les dernières actus

- ▣ [Les autorités de la concurrence des Quinze approuvent Bruxelles sur le cas Microsoft](#)
- ▣ [La Fnac prépare son site de distribution musicale](#)
- ▣ [Symbian: les parts de Psion bientôt vendues à Nokia](#)
- ▣ [Opposition européenne à l'éventuelle fusion Oracle-Peoplesoft](#)
- ▣ [Les fonds de capital-risque français ont investi 838 millions d'euros dans le secteur IT en 2003](#)

[Plus d'actualités...](#)

### Dernières Opinions



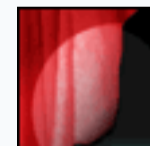
Pour un internet plus accessible aux personnes handicapées



Vingt ans de logiciels libres: quels défis pour demain?

[Plus d'opinions...](#)

### Recto Verso



Recto Verso - Docteur antivirus et Mr Hyde, iPod

désossé, sans fil et sans scrupules...

Vendredi 5 mars 2004

[Plus de Recto Verso...](#)

### Grand angle

sur l'écran du lecteur il a vu son nom, sa photo, sa fonction, son organisation, les heures de ses passages aux entrées/sorties et dans les salles de conférence.

De quoi, rajoute M. Koch, établir une cartographie complète des personnes présentes selon leurs affiliations ou affinités. Car dans ce sommet, pour la première fois la société civile était massivement représentée par des organisations et des personnes pouvant être en conflit avec leurs gouvernements, présents aussi à Genève ce qui a donné lieu à quelque ([passes d'armes éloquentes](#))

Mais Gary Fowlie est formel: «Les données des lecteurs étaient effacées à la fin de chaque journée. Seule la base de données d'accréditation des participants a été conservée, comme dans toute manifestation [de l'IUT], et sera transmise à Tunis», lieu du prochain sommet en décembre 2005.

«Notre but, souligne finalement Stéphane Koch, c'est que l'UIT ait une politique d'utilisation des données personnelles clairement définie et que ses personnels soient formés au maniement de données sensibles.»

► [Retour à Actualités](#)



▼ sponsor

**voire adresse  
@yahoo.fr**

## En savoir plus

- [Bientôt des greffes de puces RFID pour payer sans compter?](#)
- [La Cnil met les RFID et les fichiers de mauvais payeurs sur sa liste noire](#)
- [RFID: des étiquettes sous surveillance](#)
- [Des solutions pour protéger le consommateur face aux "étiquettes intelligentes"](#)

### TALKBACK



Réagissez à cet article.

- [En Belgique l'on distribue déjà des cart... \(03/03/2004\) Anonymous](#)
- [Voilà ce qui nous attends ! Plus du tou... \(23/12/2003\) Grand Frère](#)

## Comparer les prix avec ZDNet

Appareils photo numériques [Canon PowerShot A80](#)  
 Portables [Nokia 6600](#)  
 Assistants personnels [Dell Axim X3](#)  
 Logiciels [Norton Antivirus 2004](#)  
 Assistants personnels [Palm Tungsten T3](#)

Ordinateurs portables - [Dell Precision M60](#)  
 Ordinateurs de bureau - [Dell Dimension 2400](#)  
 Imprimantes - [HP DeskJet 1220c](#)  
 Baladeurs MP3 - [iRiver iHP-120](#)  
 Graveurs CD-DVD - [Sony DRU 510AK](#)

## Liens annonceurs


- [Unix contre Linux: la stratégie SCO change de cap](#)
- [L'année 2003 en revue](#)
- [Novell se raccroche au logiciel libre](#)
- [RFID: des étiquettes sous surveillance](#)
- [Brevets, logiciels et polémiques](#)

[Plus de dossiers...](#)

## Newsletters

[ZDNet News](#)

[ZDNet News Hebdo](#)

[Plus de newsletters...](#)

► [ZDNET](#) ► [ACTUALITÉS](#) ► [TECH UPDATE](#) ► [BUILDER](#) ► [PRODUITS](#) ► [TÉLÉCHARGER](#) ► [SHOPPING](#)

Services : [Newsletters](#) | [Les logiciels gratuits](#) | [ZDNet sur PDA](#) | [Plan du site](#)

## RFID: les badges du sommet de Genève avaient des effets seconds



**Le sommet mondial de la société de l'information, organisé à la mi-décembre à Genève par l'Union internationale des télécoms, a caché un détail important à ses participants. Leur badge contenait une puce électronique ou RFID, outil de traçage potentiel.**

Des puces RFID (Radio Frequency Identification) permettant de tracer le déplacement des objets ou des personnes étaient intégrées dans les badges des participants au Sommet mondial de la société de l'information (SMSI). Tous les participants (presse, société civile, industriels comme délégués officiels), et sans qu'ils en soient correctement avertis, ont reçu ces badges "sans contact" comme sésame pendant les trois jours du sommet.

L'information a été dévoilée le 10 décembre par trois universitaires et experts européens en sécurité informatique, qui ont étudié leurs propres badges. Ils ont la forme d'une carte de crédit, portant le nom du participant et une photo numérisée, prise sur place. Selon Stéphane Koch, consultant en cybercriminalité et, par ailleurs, président du chapitre suisse de l'Internet Society de Genève, le haut niveau de sécurité d'accès n'était pas garanti comme promis: on pouvait facilement s'inscrire sous une fausse identité et les photos, ne portant pas de marquage par hologramme, étaient facilement interchangeables. Ces puces ont été fabriquées par Sport Access, filiale de Kudelski, la société qui produit notamment les décodeurs de Canal Plus.

### La loi suisse imposait à l'UIT d'informer les participants

Rappelons brièvement que ces puces radio (surnommées par leurs détracteurs des "PeRFIDes") contiennent chacune un numéro identifiant unique, radiotransmis automatiquement à tout lecteur situé dans un rayon de 2 centimètres à 2 mètres.

Mais il y a plus grave, poursuit Stéphane Koch: l'Union internationale des télécoms (UIT – l'organisateur du SMSI), «aurait du avertir les participants qu'ils se baladaient avec une puce moucharde autour du cou». D'autant qu'en Suisse, la loi sur la protection des données lui imposait cette démarche.

Gary Fowlie, directeur du service communication de l'UIT à Genève, réagit pour ZDNet à ces accusations: «Les lecteurs étaient très en vue et [placés] uniquement aux points d'entrée, comme à celui de la zone VIP» dit-il. Le rayon d'action des lecteurs «était limité à 2 centimètres», ce qui suppose en effet que le participant devait s'approcher près du lecteur pour entrer, évitant ainsi d'être "scanné" à son insu. Fowlie assure enfin: «Il n'y a pas eu de tracking des participants.»

### Les données des lecteurs effacées chaque soir

Alberto Escudero-Pascual, chercheur en sécurité à l'Institut royal de Stockholm, est sceptique: sur l'écran du lecteur il a vu son nom, sa photo, sa fonction, son organisation, les heures de ses passages aux entrées/sorties et dans les salles de conférence.

De quoi, rajoute M. Koch, établir une cartographie complète des personnes présentes selon leurs affiliations ou affinités. Car dans ce sommet, pour la première fois la société civile était massivement représentée par des organisations et des personnes pouvant être en conflit avec leurs gouvernements, présents aussi à Genève ce qui a donné lieu à quelque (passes d'armes éloquentes)

Mais Gary Fowlie est formel: «Les données des lecteurs étaient effacées à la fin de chaque journée. Seule la base de données d'accréditation des participants a été conservée, comme

dans toute manifestation [de l'IUT], et sera transmise à Tunis», lieu du prochain sommet en décembre 2005.

«Notre but, souligne finalement Stéphane Koch, c'est que l'UIT ait une politique d'utilisation des données personnelles clairement définie et que ses personnels soient formés au maniement de données sensibles.»

Liens:<http://www.zdnet.fr/actualites/technologie/0,39020809,39134545,00.htm>

2003/12/24 14:15:35.653 GMT


Christine Tréguier

source: ZDnet France



afnet: <http://www.afnet.fr>

powered by zope

 <p>Club suisse de la presse GENEVA PRESS CLUB</p>	
<a href="#">Au sujet du CSP</a>	<a href="#">Prestations</a> <a href="#">Membres</a> <a href="#">Adhésion</a> <a href="#">Contact</a> <a href="#">Liens</a> <a href="#">Home</a>
<b>Prochaine manifestation</b>	
<p>106, route de Ferney 1202 Genève Tél: 022/918 50 40 Fax: 022/918 50 43 <a href="mailto:Secretariat@csp.ge.ch">Secretariat@csp.ge.ch</a></p>	<p><b><i>Invitation to the press</i></b> <b><i>and all of the members and partners of the Club</i></b></p>
<b>COMITÉ D'HONNEUR</b>	<p>The <b>Geneva Press Club - Club suisse de la Presse</b>, in collaboration with <b>Internet Society Geneva</b>, has the pleasure to invite the international and the Swiss press to a press meeting on the topic</p>
<p><b>SIR PETER USTINOV</b> Ecrivain, Bursins, Président <b>LAURENCE DEONNA</b> Reporter et écrivain Genève <b>MARCEL A PASCHE</b> Directeur honoraire, Edipresse, Lausanne <b>SEYMOUR TOPPING</b> Adm., Prix Pulitzer, New York <b>ROLF ZINKERNAGEL</b> Prix Nobel, Zurich</p>	<p>World Summit on the Information Society</p> <p><b>How data collection from the organizers threatens Civil Society's privacy</b></p> <p>THE DATA COLLECTION AT WSIS VIOLATES THE SWISS, EU AND UN DATA PROTECTION GUIDELINES</p> <p><b>Friday 12th December 2003 at 11.30 a.m.</b></p> <p>à " la Pastorale ", <a href="#">Route de Ferney 106</a></p>
<b>MEMBRES " médias "</b>	
<p>Agefi Groupe, AJI, Animan, ATS, Bloomberg News, Bluewin, Construire, Coopération, La Côte, Edipresse, FSJ, GHI, Le Courrier, Le Temps, Léman Bleu Télévision, L'Extension, L'Express, L'Impartial, La Liberté, Le Nouvelliste, Naville SA, Promoédition, Publi-Annonces, Publicitas Léman, Radio Lac, Ringier romandie, RSF, RSR, Salon du Livre et de la Presse, SGA, Swissinfo-SRI SSR/SRG, TA-Media AG, 022 TéléGenève, Tribune de Genève, TSR, UER</p>	<p>An International group of independent researchers attending the World Summit on the Information Society (WSIS) has discovered important technical and legal flaws in the security system used to control access to the UN Summit.</p> <p>The system not only fails to guarantee the promised high levels of security but also introduces the very real possibility of constant surveillance of the representatives of the civil society breaking the European, Swiss and UN conventions in data protection.</p> <p>During the press conference we will explain how the system fails to guarantee the promised high levels of security and introduces a real threat for the representatives of civil society, many of whom are critical of certain governments and regimes.</p> <p>That a system like this gets implemented without a transparent and open discussion amounts to a real threat for the participants themselves, and for our Information Society as a whole.</p> <p><b>Website:</b> <a href="http://www.contra.info/wsiv">http://www.contra.info/wsiv</a></p> <p><b>SPEAKERS:</b></p> <p><b>Ass. Prof. Dr Alberto Escudero-Pascual</b>, Researcher in Computer Security and Privacy, Royal Institute of Technology, Sweden (English, Spanish) Tel: + 41 796075733, +46 702867989</p>

**MEMBRES  
" collectifs "  
et principaux  
partenaires**

Confédération suisse, Etat de Genève et Ville de Genève, Aéroport International de Genève, Air France, Assoc. PME, British American Tobacco, Banque Piguët, Banque cantonale de Genève, BIT, CAII, CDE, CERN (Assoc. du pers.), CICR, CIO, Collège du Léman, Course de l'Escalade, Devillard, Eden Springs, economiesuisse, EMA, Euro RSCG, Euroscience Léman, Finartis, First Tuesday FSP, Fondation Bertarelli, Fondation pour Genève, FAID, Geneva Coalition, Groupement des Banquiers privés genevois, GSCGI, Hôtel Bristol, Hôtel Intercontinental, Ibéria, Internet Society Geneva, IUCN, Japan Tobacco International, Journal des Cafetiers romands, Loterie romande, Mission d'Angola, Mission de Russie, Office espagnol du tourisme, OIF, OMPI, OMS, Orbital, ORGEXPO, Pen Club suisse romand, Philip Morris, Reporters sans Frontières, Serono, Shandwick, SRRP, Swiss, TCS, Telehouse (Suisse) SA, TPG, Trimedia, UEFA, Union Bancaire Privée, Victorinox, World Economic Forum

**George Danezis**, Research in privacy enhancing technologies and computer security, Cambridge University, UK (French, Greek, English)

**Stephane Koch**, President Internet Society, Executive Master of Economic Crime Investigations (French, English)

Tel: +41 79 607 57 33

Au plaisir de vous revoir à cette occasion.

Guy Mettan, Directeur exécutif

