

Privacy Digest

Your daily source for news that can impact people's privacy.

php view

view ('zone:5', 0, '', '', '0');

Search for this:
WEBINATOR COPYRIGHT © 1995-1998 THUNDERSTONE - EPI, INC.

March 2004

Sun	Mon	Tue	Wed	Thu	Fri	Sat
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			

Feb Apr



- **More News**
[Wired News](#)
[Washington Post](#)
[Robert O'Harrow Master.com](#)
[Yahoo! News](#)
[Tech Law Journal](#)

Monday, March 8, 2004

- [New York Times](#) - free registration required [Justices Hear Arguments on Internet Pornography Law](#).

WASHINGTON, March 2 -- The [Supreme Court](#) heard oral arguments on Tuesday about Internet pornography, one of the most vexing issues at the intersection of technology and [First Amendment](#) rights.

Neither side got a free ride from the justices in the discussion of the "Child Online Protection Act", a 1998 law that makes it illegal for commercial Web sites to make available to children 16 and under material that is not necessarily obscene but could be considered "harmful to minors" under a complex, three-part formula in the law.

view ('zone:4', 0, '', '', '0');

- [CNET NEWS.COM](#) - [Microsoft wants to know who your friends are](#).

To try to translate that idea into digital terms, Cheng and her team have come up with a concept called Inner Circle, which automatically maintains and updates a list of about 20 people with whom one is e-mailing and instant messaging the most.

The project is one of several efforts Cheng's team showed off this week at Microsoft's TechFest. The two-day event brings thousands of company employees to the giant's headquarters in Redmond, Wash., to hear presentations from workers in Microsoft Research's five labs, based in Cambridge, Mass., the Silicon Valley, San Francisco, Redmond and Beijing.

- [MIT's Technology Review](#) - [Losing Control of Your TV](#). By [Simson Garfinkel](#)

The latest anti-piracy move will prevent you from making high-quality copies of broadcast TV programs. And the new "broadcast flag" technology enables all manner of other restrictions.

In the future, the [Motion Picture Association of America](#) will control your television set. Every TV sold in the United States will come equipped with an electronic circuit that will search incoming TV programs for a tiny electronic "flag." The MPAA's members will control this flag, putting it into broadcast movies and television shows as they see fit. If the flag is present, your TV will go into a special high-security mode and lock down its high-quality digital outputs. If you want to record a flagged program, you'll have to do so on analog tape or on a special low-resolution DVD. Any recording will be limited to analog-quality sound. This security measure is not designed to protect the television from viruses or computer hackers--it's designed to protect TV programs from you.

This future arrives on July 1, 2005.

Legally known as the Advanced Television Systems Committee Flag, but better known as the broadcast flag, this little bit of Machiavellian technology was folded into the [Federal Communications Commission's](#) rulebooks last November. Reaction since then has been mixed. Most journalists writing about the flag have said that it won't affect most consumers--unless they try to record high-quality digital video in their living room and play it back in their bedroom. The Center for Democracy and Technology called the FCC's ruling a historic compromise that will preserve many consumer rights while preventing rampant video piracy as television goes digital, but [CDT](#) also notes that the FCC's whole process for approving the broadcast flag sets a dangerous precedent that could easily turn against consumers. Indeed, many technologists that I've spoken with believe that the broadcast flag introduces dangerous Trojan Horse technology--a technology that could be rejiggered with even stronger anti-consumer provisions as time goes on. "Any broadcaster who uses it should lose their license because it is a misuse of the public's trust," says Andrew Lippman, a senior research scientist at the MIT Media Lab.

view ('zone:6', 0, '', '', '0');

« [webloggers](#) »

In fact, all of these things are true.

- [PCWorld.com](#) - [Experts Question Microsoft's Caller ID Plans](#).

Is the software giant trying to profit from the proposed e-mail security system?

Just a week after Microsoft's Chairman and Chief Software Architect Bill Gates unveiled a plan for securing e-mail communications, leading e-mail authorities, legal experts, and at least one Internet service provider are expressing concerns about the e-mail sender authentication plan, known as Caller ID.

Some experts agree that the technology is promising. However, Microsoft's claim that it owns patents around Caller ID and its decision to license the technology to third parties, rather than submit it to an Internet standards body, have riled e-mail experts and domain owners, some of whom say they worry about a power grab by the Redmond, Washington, company and are wary of signing on to the new system.

- [SiliconValley.com](#) part of San Jose [Mercury News](#) - [This Is Your Life](#).

Recorder Can Be Worn Around The Neck To Provide A Photo Diary Of Your Entire Day

[...]

It begins with the SenseCam, a device Microsoft researcher Lyndsay Williams calls "a black box recorder for the human body." SenseCam was one of dozens of new technologies on display this week at [Microsoft's TechFest](#), an annual event to give employees a look at the company's research around the world.

Hidden inside a piece of jewelry or badge, the SenseCam records hundreds of images a day without the wearer ever pressing a button. The fish-eye lens faces forward, taking pictures of the scene in front of the person wearing it.

Fusing a digital camera with a variety of small sensors, the SenseCam's shutter is triggered by any change in motion, light or temperature. Later, Microsoft might add sensors that detect sound and heart rate.

- [Slashdot](#) | [Your Rights Online](#) - [Australia-U.S. Trade Agreement Contains DMCA-like Provisions](#).

view ('zone:8', 0, '', '', '0');

Archive by date

1997	1998	1999
2000	2001	2002

Open links in new window

- **PrivacyDigest.com**

- [Home page](#)
- [Support this site](#)
- [Hire the editor](#) **NEW**
- [Link to us](#) **NEW**
- [Privacy Digest Store](#) **UPDATED**
- [Syndication\(XML/RSS\)](#)
- [Privacy Digest - FAQ](#)
- [Privacy Policy](#)
- [Search Site](#)
- [Poll - Features](#)
- [Poll - Donations](#)
- [Mailing list](#) **NEW**
- [Mailing List \(old\)- Announce](#)

- **Translate into:**
[French, Spanish, German,](#)
[Italian, Portuguese](#)

view ('zone:9', 0, '', '', '0');

- Discussion area disabled for now
Coming Back soon

Warning: main(httpdocs/static/include/c open stream: No such file or directory in [/home/httpd/vhosts/PrivacyDigest.com](#) on line 591

Warning: main(): Failed opening 'httpdocs/static/include/discuss.php' for i (include_path=.:usr/share/pear) in [/home/httpd/vhosts/PrivacyDigest.com](#) on line 591

- **Support Privacy Digest**



[Our Amazon Wish List](#)

rate me on [BlogHor](#)
 [help?](#)

Other Projects

- [MacRonin Gaming](#)
- [NewsLogs Magazines](#)
- [Lots Of Tools](#)
- [Lots Of Housewares](#)
- [Lots Of Children's Books](#)
- [Lots Of Good Movies](#)
- [Lots Of Computers](#)
- [Lots Of Cool Electronics](#)
- [Lots Of Things For Baby](#)
- [Lots Of Toys](#)
- [Lots Of Photography](#)
- [Lots Of Clothing](#)
- [Lots Of Software](#)

femto writes "The [text](#) of the US-Australian Preferential Trade Agreement has been released. It has significant [implications](#) for Free Software and the Public Domain within Australia. Implications include extension of copyright terms (death to the Public Domain & [Gutenberg Australia](#)), software patents (death to Free Software) and the DMCA (death to fair use). It is not yet law. The [Europeans](#) have shown that software patents are not a done deal. Now is the time to write letters to members of the [House of Representatives](#) and the [Senate](#). Join the [EFA](#). Contact your local [library](#). Sign up to the [mailing list](#) to organise opposition. Just make a noise during this year's [federal election](#)."

- Political News from [Wired News](#) - [ISP Files First Can-Spam Lawsuit](#).

A California Internet service provider is putting the federal Can-Spam Act to its first test, two months after the law passed, by filing a lawsuit against the owner of home-improvement website BobVila.com.

Hypertouch, based in Foster City, California, filed the suit on Thursday claiming the owner of BobVila.com and its marketing affiliate BlueStream Media violated provisions of the Can-Spam Act by sending out e-mail advertisements containing missing contact information. The suit claims that BlueStream Media forged the header information that can help e-mail recipients identify where a message originated.

- [Slashdot](#) | [Your Rights Online](#) - [First CAN-SPAM Lawsuit Filed in California](#).

[rocketjam](#) writes "Foster City, California-based ISP Hypertouch, Inc. has [filed the first lawsuit alleging violations of the new Federal CAN-SPAM Act of 2003](#). The lawsuit was filed against BobVila.com and the spammer they hired, Bluestream Media, for sending Hypertouch customers unwanted, unsolicited email advertisements for Vila's "Home Again Newsletter." [The suit alleges](#) the defendants sent spam email ads with fraudulent headers and no physical address. It also alleges the emails were sent to randomly generated and harvested addresses as well as addresses that had replied to opt-out links in other spams. Hypertouch's attorney, John L. Fallat, said the CAN-SPAM Act offers little protection to the public, but they would use the few protections it offers to punish spammers." --- Reader Clemence links to [Wired's coverage of the suit](#).

- San Jose [Mercury News](#) - [Background-check kit hits retail shelves](#).

NEW YORK (AP) - Beyond the gallon jars of mayonnaise and the office furniture, shoppers browsing the aisles at some Sam's Club stores will find something that isn't usually sold at retail -- an employee background check in a box.

"Make better hiring decisions," says the package, a little smaller than a box of breakfast cereal. "Conduct background checks quickly and easily!"

With security-conscious employers stepping up scrutiny of job candidates, background checks have become standard procedure at many companies.

But the new check-in-a-box, which is marketed by ChoicePoint Inc. and began selling alongside software for \$39.77 late last year, points to new efforts by data vendors to market background screening as a consumer product.

ChoicePoint -- with nearly \$800 million in annual revenues, one of the nation's largest vendors of personal, financial and legal data -- also recently began selling background checks via Yahoo's HotJobs.com online employment board, offering jobseekers the chance to vet themselves. Entersect, owned by competing data provider LocatePlus Holdings Inc., says it plans to launch a self-check service later this year on CareerBuilder.com.

[...]

ChoicePoint, though, says it has built strong safeguards into its system to avoid privacy breaches. But they are not absolute.

For starters, there's the sticker that seals the top of the box. "Business License Required," it reads.

In practice, however, a purchaser can use most of the screening options -- including criminal background checks, Social Security number identification and vetting of credentials -- without supplying such a license, ChoicePoint acknowledges.

[...]

Searching background information with the new check is pay-as-you-go. Buying the ChoicePoint product requires having a \$30 membership at Sam's Club, as well as shipping costs if ordered online. It comes with \$50 credit for searches -- enough to run a national criminal check, identity verification, and employment verification on one person, as well as a drug test.

Additional checks cost from \$3 to verify a Social Security number to \$9 for a credit report to \$25 for a national criminal screening.

- [Slashdot](#) | [Your Rights Online](#) - [Background-Check Software Goes Retail](#).

Makarand writes "According to this article in the Mercury News, [ChoicePoint Inc.](#), one of the nation's largest vendors of personal, financial and legal data is attempting to [mass market a background-check software tool-kit](#) which can be used to tap into ChoicePoint's online databases. Choicepoint requires that you have a business license to run a small business to use this software. However, as users of these services are rarely audited or asked to produce their business license, the purchaser can potentially conduct criminal background checks, Social Security number identification and other checks on anyone for a small fee. Privacy advocates are cautioning that making background-check software a consumer product could easily put personal information into the wrong hands."

- [New York Times](#) - [free registration required In Texas, Hire a Lawyer, Forget About a Doctor?](#)

As domestic security director for 16 north Texas counties, Greg Dawson of Fort Worth has many dealings with doctors and hospitals, preparing for a terrorism emergency he hopes will never come.

So, Mr. Dawson said, he was stunned this week to find that his name had been added to a little-known Internet database for doctors attacking "litigious behavior." His offense: filing a medical malpractice lawsuit against a Fort Worth hospital and doctor over the death of his 39-year-old wife, whose brain tumor was missed, and winning an undisclosed settlement.

[Lots Of Video Games](#)
[Privacy Digest Store](#)
[Lots Of Great Sites](#)
[Lots Of Good Music](#)
[Classical, Popular](#)
[Lots Of Good Books](#)
[Biography, Law,](#)
[Medical, Romance](#)
[Lots Of Information](#)
[CIA World Fact Book](#)
[CIA Intelligence Bk2002](#)

view (zone:10', 0, ", ", '0');



For months, an obscure Texas company run by doctors has been operating a Web site, DoctorsKnow Us.com, that compiles and posts the names of plaintiffs, their lawyers and expert witnesses in malpractice lawsuits in Texas and beyond, regardless of the merit of the claim.

[...]

The sponsors draw no distinctions among cases in what they say is the first effort to use public sources to compile a list of litigants in "predatory lawsuits" that are causing a medical crisis. One couple was put on the list after winning \$40.9 million over a botched operation by a drug-dependent surgeon.

Mr. Dawson said he recently had trouble finding a doctor for his son and considered it possibly retaliatory. "I thought how amusing, I'm blacklisted," he said.

He said he learned he was on the list from Texas Watch, a consumer research and advocacy organization based in Austin.

[...]

The "American Medical Association" said that it had just learned of the group and that it saw no ethical issues at stake.

- Slashdot | [They Can Sue, But They Can't Hide](#).

An anonymous reader writes "The New York Times (free reg's yada, yada) has [this article](#) about Texas doctors running an online blacklist of patients who have sued. The searchable database is at [doctorsknow.us](#). Nice to know that you can get blacklisted for suing the doctor that caused massive brain damage to your kid (and winning)." --- To add a plaintiff to the database, [membership was not always required](#).

Thursday, March 4, 2004

- Avi Rubin - [My experience as an Election Judge in Baltimore County](#).

It is now 10:30 pm, and I have been up since 5 a.m. this morning. Today, I served as an election judge in the primary election, and I am writing down my experience now, despite being extremely tired, as everything is fresh in my mind, and this was one of the most incredible days in my life.

I first became embroiled in the current national debate on evoting security when Dan Wallach of Rice University and I, along with Computer Scientist Yoshi Kohno and my Ph.D. student Adam Stubblefield released a [report](#) analyzing the software in Diebold's Accuvote voting machines.

- Slashdot | [Your Rights Online - Avi Rubin's Thoughts On e-Voting](#).

[nazarjo](#) writes "Avi Rubin, a well regarded Johns Hopkins computer science professor and leading critic of e-voting, has written an [account of his experience as an election judge](#) on super tuesday. Maryland was experimenting with e-Voting machines. Rubin puts it this way, 'this was one of the most incredible days in my life.' He wrote his experiences immediately after the day was over, capturing his perspective on the subject. A very interesting read."

- Slashdot | [MSN Search Blocking Results For XFree86?](#)

[Peacefire](#) writes "Thomas Shaddock spotted this on <http://www.root.cz/> (in Czech) -- if you go to <http://search.msn.com/> and search for 'XFree86', it tells you that you've 'entered a search term that is likely to return adult content', and directs you to the porn search engine NightSurf.com, which lists a bunch of porn sites that ostensibly match the term 'XFree86'. If you search for 'XFree86' on Google, however, it's clear that the top matching terms returned by a normal search, are XFree86 sites, are not a bunch of porn sites. MSN is apparently blocking the specific term 'XFree86' and not just filtering on something stupid like the 'X' or the 'Free', since you can search for 'XFree85' and 'XFree87' with no problem. And search terms like 'Linux', 'AOL' and 'Macintosh' are allowed, so at least MSN hasn't simply blacklisted all competitors' keywords as 'porn', but why would they be blocking 'XFree86'?"

- Washington Post via Yahoo News - [FCC Rule on Local Phone Service Rejected](#).

A U.S. appeals court yesterday struck down key elements of a [Federal Communications Commission](#) rule governing local telephone competition, handing a major legal victory to the regional telecom giants as they attempt to ward off insurgent rivals.

If implemented, both sides in the debate said, the decision would put in jeopardy an eight-year-old system that allows competitors to lease phone networks owned by large local carriers such as Verizon Communications Inc. at government-mandated rates.

In a 3-0 ruling by the D.C. Circuit Court of Appeals, the judges wrote that the FCC lacks the authority to delegate responsibility for setting those rates to the states. The court also ruled the FCC had failed to prove that competitors in the local phone market are "impaired" without government-regulated access to critical parts of the phone network controlled by the regional giants.

The ruling, scheduled to take effect in 60 days, represents the latest chapter in a long-running debate over what kind of government safeguards are needed to ensure consumers have a choice in their phone service. The matter has now been kicked back and forth between the courts and the FCC several times.

In their written opinion, the judges lashed out at the FCC for its "failure, after eight years, to develop lawful . . . rules, and its apparent unwillingness to adhere to prior judicial rulings."

- Slashdot | [Your Rights Online - Courts Overturn FCC - Return of the Monopoly?](#)

An anonymous reader writes "The DC Circuit Court of Appeals today [threw out FCC restrictions](#) which previously forced large regional phone companies to allow companies such as AT&T and MCI the ability to offer local phone service. The court also upheld FCC rules that no longer require large phone companies to share their advanced broadband networks of the future with competitors. The [USTA response](#): 'This is a decisive victory for consumers, for innovation and for free markets.' The [AT&T response](#): 'At a time when consumers and small

business owners are just beginning to realize the benefits of competition, the D.C. Circuit today held up a stop sign and halted eight years of progress.' Enough about the Baby Bells already -- how is this going to effect my VoIP phone from [VoicePulse](#) (similar to [Vonage](#))? Did I switch to VoIP so I can pay \$15/month for my phone bill, but will have to pay \$80/month for [FTTH](#) or some other form of broadband?"

Wednesday, March 3, 2004

- InfoStructure News from [Wired News](#) - [Another Virus to Worry About](#).

There's another worm loose on the land -- Netsky-D. It arrived by e-mail on Monday and, while not especially damaging, it's a pain to get rid of.

- Medical Technology News from [Wired News](#) - [Bioethics Shuffle Ignites Outcry](#).

Members of President Bush's Council on Bioethics will likely play nice now that they all agree on embryonic stem-cell research and cloning. But they aren't an accurate representation of American citizens, critics say.

[...]

President Bush's decision to replace two members of his bioethics panel with three appointees whose beliefs are closer to his own has sparked a new round of criticism on how the administration handles science.

- [A new e-mail virus making the rounds](#)

It seems there is a new one making the rounds. This one claims to come from your ISP/companies e-mail support people. The two variations I have received so far were titled "Notify about using the e-mail account." and "E-mail account disabling warning." Each has a PIF file attached that you are supposed to read for an explanation. The text content of each follow:

```
Subject: Notify about using the e-mail account.
Parts/Attachments:
1 Shown 10 lines Text
2       12 KB  Application
-----
```

Hello user of PrivacyDigest.com e-mail server,
Our main mailing server will be temporary unavailable for next two days, to continue receiving mail in these days you have to configure our free auto-forwarding service.

For details see the attached file.

Cheers,
The PrivacyDigest.com team
<http://www.privacydigest.com>

[Part 2, Application/OCTET-STREAM (Name: "Information.pif") 16KB.]

The second said:

```
Subject: E-mail account disabling warning.
Parts/Attachments:
1 Shown 10 lines Text
2       12 KB  Application
-----
```

Hello user of PrivacyDigest.com e-mail server,
Your e-mail account will be disabled because of improper using in next three days, if you are still wishing to use it, please, resign your account information.

For more information see the attached file.

Best wishes,
The PrivacyDigest.com team
<http://www.privacydigest.com>

[Part 2, Application/OCTET-STREAM (Name: "Information.pif") 16KB.]

And I obviously know that I did NOT send ether of these e-mails.

- "Network World Fusion" - [Doubts dog Microsoft spam plan](#).

Even with Microsoft lending its clout to an expanding anti-spam movement centered on authenticating e-mail senders, experts caution the approach comes laden with technical challenges and unanswered questions.

The software giant last week published its Caller ID for E-mail specification, which lays out how to thwart the spoofing of e-mail addresses, a popular spammer trick. The specification, which Microsoft hopes will become a standard, is the first piece of the company's long-term spam-fighting strategy called the Coordinated Spam Reduction Initiative (CSRI), which also was introduced last week at the annual RSA Conference in San Francisco.

- [eWeek - Spam Tide May Be Turning](#).

Major announcements at the RSA Conference here last week--in addition to recent anti-spam technology advances--mark the beginning of the end of spam as we know it.

At the conference, [Microsoft](#) Corp. introduced its CSRI (Coordinated Spam Reduction Initiative), and Sendmail Inc. announced broad support of SMTP identification schemes.

Other anti-spam initiatives have moved ahead in recent weeks. The SPF (Sender Policy Framework), championed by Meng Weng Wong, gained traction on the news that it will be formally submitted to the Internet Engineering

Task Force. [Yahoo](#) Inc.'s Domain Keys, announced in December, has also bolstered the campaign for e-mail identity technology. Brightmail Inc.'s Reputation Service and IronPort Systems Inc.'s SMTPi initiative debuted late last month as well.

The premise of these new tools and initiatives is that once identity is effectively tied to e-mail messages, mail-handling systems will be able to forward legitimate e-mail and trash the forged junk now flooding the Internet.

eWEEK Labs therefore recommends that IT managers focus their energy on implementing new technology in their e-mail systems, instead of evaluating content-filtering anti-spam tools.

Tuesday, March 2, 2004

- [Yahoo News - E-Voting Terminals Face Super Tuesday Test.](#)

WASHINGTON (Reuters) - Maryland's sleek new voting machines will be swathed in tamper-proof tape during Tuesday's primary election, but that won't make computer scientist Avi Rubin any more confident in the outcome.

- [BBC NEWS | World | South Asia | Gearing up for India's electronic election.](#)

Over one million voting machines will be rolled out for the polls

Technicians are working overtime to make India's first all-electronic general election go smoothly.

The task is a challenging one in this one-billion-strong nation - the world's largest democracy - where most voters are still poor, rural workers.

Over one million electronic voting machines (EVMs) are required to cover this vast nation, from the Himalayas down to Kanyakumari on the southern tip.

- [Slashdot | Evoting in India, Maryland.](#)

[Anonymous Coward](#) writes "EVMs are back in the news again. The BBC is reporting on the use of [over a million Electronic Voting Machines \(EVM\) in India](#) for Parliamentary elections in April. With a billion people and an electorate of 668 million, it is by far the largest democratic election exercise in the world. A picture of an EVM is provided." --- And Kierthos writes "An [article](#) on Yahoo! News mentions that Maryland's voting terminals will be wrapped in tamper proof tape, which 'just protects that malicious code physically', according to computer scientist Avi Rubin. Also mentioned are California's ongoing system of e-voting, as well as a point on whether Diebold should be banned in California after using uncertified software in last October's election."

- [Slashdot | Hackers: The Art of Abstraction.](#)

[scubacuda](#) writes "[Wired](#): Inspired by [McKenzie Wark's The Hacker Manifesto](#), Madrid's [MNCARS's](#) exhibit, [Hackers: The Art of Abstraction](#), explores the connections between hackers, artists and anyone engaged in any kind of creative work. The centerpiece of the exhibition are documentary films and videos made by independent filmmakers and hackers from all over the world, including [Freedom Downtime](#) by Emmanuel Goldstein, Free Radio by Kevin Kayser, The Hacktivist by Ian Walker, Unauthorized Access by Annaliza Savage, New York City Hackers by Stig-Lennart Serensen and [Hippies From Hell](#) by Inne Pope."

- [The Register \(UK\) - UUNet tops spammer-hosting super league.](#)

UUNet hosts more spammers than any other ISP. It has 151 listings on the Spammers Block List (SBL), including 34 known spam gangs with ROKSO records, according to the anti-spam organisation "Spamhaus" records for February 2004.

"The second worst offender, Chinanet-QD, has 82 entries on the SBL. It hosts Alan Ralsky, listed as the single worst spammer on the ROKSO list."

- [Slashdot | Your Rights Online - UUNet Is The Number 1 Spam Host.](#)

An anonymous reader submits "Statistics for February have UUNet leading the Spamhaus [top 10 worst Spam ISPs](#) chart. [The Register](#) point out that ISPs like UUNet and Abovenet continue to host spammers despite advertising anti-spam AUPs." --- And the competition is probably wishing they had as much luck.

- [Slashdot | FreeS/WAN Project Bows Out.](#)

V. Mole writes "After five years, the [FreeS/WAN](#) project has decided to [end development](#). The main reason seems to be that although the project was technically successful, it was not making much progress with its [political goals](#) of encrypting a significant portion of all Internet communications, although one might guess that the selection of KAME for the standard Linux IPSEC implementation might also have influenced this decision. And don't panic, the software will remain available, and of course some other group is free to continue development."

Saturday, February 28, 2004

- [Business News from Wired News - Germans Protest Radio-ID Plans.](#)

Activists protesting in Germany manage to force a giant retailer to backtrack this week on some of its plans to collect consumer data. But activists say the company didn't go far enough.

[...]

Led by German privacy organization FoeBud, activists in Rheinberg, Germany, plan to stage a protest outside the Metro Extra Future Store, a department store that serves as a site to test RFID tracking and other retailing technologies.

Metro AG, the store's parent company, is the world's fifth-largest retailer with more than 2,000 stores, including supermarkets and electronics stores in 28 countries.

Activists recently discovered RFID chips embedded in the store's customer loyalty cards. They also found them in products for sale there, including goods from IBM, Gillette and Procter & Gamble. Metro failed to notify customers that they were being tracked. Although Metro told activists the chips worked only while customers were inside the store, activists discovered that a kiosk used to deactivate the chips didn't completely disable the tags.

An RFID tag consists of a microchip the size of a grain of sand attached to an antenna that transmits information whenever it passes in front of an RFID reader. Product manufacturers and stores have expressed interest in placing the tags on consumer items to manage inventory, track consumer interest, speed checkout time and thwart thieves.

Critics say the tags would let businesses monitor the movement of citizens and collect information for marketing purposes. Information transmitted by the tags can be read up to 10 feet away.

Public outcry and the impending protest over the privacy violation at Metro forced the company to cancel its use of RFID tags in loyalty cards. The company announced Thursday it would cease embedding RFID chips in its loyalty cards and would replace cards that were already distributed to customers.

"This demonstrates the power of the free market at work," said Katherine Albrecht, director of Consumers Against Supermarket Privacy Invasion, or [CASPIAN](#), an organization based in the United States. "The world's people are telling global businesses ... that they won't tolerate being spied on through products and services."

Even with Metro's retreat, representatives from 14 privacy and civil rights organizations in Germany said they would proceed with the Saturday protest. Rena Tangens, founder of FoeBud, said the announcement didn't go far enough since the company and its product partners didn't agree to remove tags from products.

- [Detroit Free Press - Ford device intended to unclog roads.](#)

The experiment is intended to turn vehicles into mobile traffic-monitoring tools. They'll report their locations and speeds along with road temperatures, whether their headlights and windshield wipers are activated, even if their antilock braking systems have been used.

Slow vehicle speeds with frequent stops would signal traffic congestion, for instance. Windshield use along with near-freezing pavement temperatures and ABS activations would point to slick conditions.

Currently, traffic and weather are monitored by satellites and sensors on highways. The data are not detailed enough to prevent traffic jams.

"We are trying to develop the next-generation travel advisory system," said Ron Miller, project leader for intelligent vehicle technologies at Ford's research and advanced engineering unit in Dearborn.

- [Slashdot | Ford Testing a New 'Traffic Monitoring' Device.](#)

[Poletown](#) writes "The Detroit Free Press put out this article today about a new [vehicle based 'traffic monitoring' system](#) that Ford is testing. It will report your speed, the road temperature, whether or not your wipers/headlights are active, and even if you've used your anti-lock brakes. Initially, the system will be tested on Ford-owned and municipal vehicles."

- [Slashdot | Your Rights Online - Utah Leads the Way Toward RFID Privacy Legislation.](#)

An anonymous reader writes "Wired News reports that Utah's House of Representatives passed the first-ever [RFID privacy bill](#) this week, 47-23. Utah state Rep. David Hogue said that without laws to ensure consumer privacy, retailers will be tempted to match the data gathered by RFID readers with consumers' personal information. 'The RFID industry will carry the technology as far as they can,' said Hogue, sponsor of the Radio Frequency Identification Right to Know Act. 'Marketing people especially are going to love this kind of stuff.'"

- [Slashdot | Your Rights Online - DeCSS Trade Secret Case Comes to an End - Again.](#)

Andrew Bunner writes "We asked the courts to rule on our appeal of the DeCSS preliminary injunction (even though the DVD CCA dropped the case) and... we won! No more preliminary injunction. Here's the [official ruling](#) (pdf)." --- This is the last gasp of this case, which we've [been following](#) for some years now. This ruling goes into some depth analyzing the trade secret claim, gets the ruling "right", and should be helpful in future cases on similar topics.

- [Slashdot | Your Rights Online - Jail Time for Misleading Domain Names.](#)

Bootsy Collins writes "The Miami Herald is running a [story](#) on the first-ever prison sentencing (and, for that matter, prosecution and conviction) under the Federal Truth in Domain Names Act. This act, combined into the larger [Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act \(PROTECT\) of 2003](#), made it a violation of U.S. Federal law to use a misleading domain name with the intent to deceive someone into viewing obscene material -- larger penalties if attempting to so mislead minors, but up to two years even if adults are the object. In the case in question, a man was convicted for registering thousands of domain names which were close misspellings of popular web sites for kids. Attempting to surf to those sites would redirect to a site entitled 'Dorm Sex Party.' Before being arrested, the convicted typosquatter made about a million dollars for the referrals." --- He's [been on Slashdot](#) before.

- [Slashdot | Stolen Laptop Alarms.](#)

torok writes "Three Engineering students from [Simon Fraser University](#) in Burnaby, BC, Canada have developed a [laptop alarm](#) complete with remote pager that detects if your laptop is being moved and sounds an alarm. The article is a bit sketchy on details, but it sounds like a cool idea."

- [Privacy News from Wired News - Fighting for Right Not to Show ID.](#)

Next month, the [Supreme Court](#) will consider whether people have the right not to show identification to the police. At stake, advocates say, is whether our society will have to "show papers" in daily life.

[...]

Those courts upheld the conviction, but the U.S. Supreme Court agreed to review the case in October 2003.

In his first media interview in three years, Hiibel told Wired News he hoped "the [Supreme Court](#) will uphold the [Constitution](#) and the [Bill of Rights](#) and that all Americans, not just me, have the right to privacy."

"I feel quite strongly I have a right to remain silent and I didn't commit a crime," Hiibel said. "(The deputy) demanded my papers. I exerted my rights as a free American and I was cuffed and taken to jail."

Harriet Cummings, one of three Nevada public defenders working on the case, said that while the case might seem like "no big deal," the legal issues at stake are huge.

"This goes to the very nature of what our society is going to be like," Cummings said. "We believe that exercising your right to remain silent should not be something that can cause you to be imprisoned."

"If an officer acting under suspicion that a crime has been committed comes up to a person, starts asking questions and demands identification, and if the person, as Mr. Hiibel did, declines that demand, they can be hauled off to jail," Cummings said. "And we think that is not something that should happen in a free society."

© copyright 1997-2004 by [Paul Hardwick](#). All rights reserved.
All trademarks are the property of their respective owners.

Modified: 6/10/01; 1:46:02 AM
Built: 3/8/04; 3:17:07 AM

URL for current page: <http://www.PrivacyDigest.com/index.html>