Privacy Journal
AN INDEPENDENT MONTHLY ON PRIVACY IN A COMPUTER AGE
PO Box 28577
Providence RI 02908

February 2010 Volume 36, Number 4 *Electronic Edition*

IBM Develops Profiling Around Airports

One of the great holes in air-travel security is, of course, that there is virtually no screening for persons approaching and entering airports, even though screening for boarding aircraft has been tightened. Many more persons could be maimed and killed by an attack inside an airport than inside an airplane, but access remains fairly easy.

IBM has applied for at least eight patents on a sophisticated computer-analysis technique to address this, by using profiling of passengers, based on attributes such as age and type of clothing worn, and even by analyzing nervous furtive glances by individuals. The system would require a network of video, motion, chemical, and biometric sensors arrayed throughout the airport and perimeter. The sensors feed into a grid of networked computers, which provide high-powered processing to get results to security officers in so-called real time, yet the systems are compact enough to be located on-site, according to a story published last month by Alex Wolfe, editor-in-chief of InformationWeek.com.

"The 'secret sauce' in the set up is a software 'inference engine,' which crunches the data fed in by the multitude of sensors, separating the high-risk wheat from the false-alarm chaff. That engine uses heuristics and rules developed by the three co-inventors behind the patent applications – James Kraemer, Robert Friedlander, and, Robert Angell," ***InformationWeek*** reported.

Angell, a laid-off IBMer now teaching computer science at a community college near Salt Lake City, told Wolfe, "If it's done right, we could do passive profiling [and] passive detection and do it without a whole lot of fanfare."

The patent application purports that the methodology can pick up and sort out attributes like an individual's age, make and/or model of a vehicle, color of a hat, breed of a dog, sound of an engine, a medical diagnosis, medicines, date of birth, a color, item of clothing, walking, talking, running, a type of food eaten, an item purchased, smoking, walking, jogging, walking a dog, carrying bags, carrying a baby, riding a bicycle, an engine running, a baby crying, or any other event."The patent application also various-

(Continued on page four)

More on the Nude Airport Scanners

Ralph Nader, the long-time consumer activist, has turned his sights to the "backscatter" nude screening devices and other technology at airports.

"Multi-million dollar investments in intelligence failed to do its job," Nader told a group of privacy advocates gathered in Washington by the Electronic Privacy Information Center last month, and so the government is turning to untested technological fixes. He said the government was "sold a bill of goods" with regard to devices that puff air at a traveler to dislodge and detect explosive powders. "There's a commercial motivation. Vendors persuade government security agencies to purchase this stuff. I wonder if you could get a court injunction holding up procurement?" Nader questioned whether the nude screening machines emit harmful radiation to frequent travelers.

"Dragnet surveillance is the last resort of people who haven't done their jobs. Our entire homeland-security operation is made up of ad hoc responses to the last failure."

Homeland Security authorities have claimed that the body scanners do not provide details of genitals, but a journalist for ***The Guardian*** in Great Britain who attended a demonstration reported that it showed clearly that male genitals are visible in undoctored images. This month airport officials in Australia admitted this. In addition, an anonymous YouTube video shows

(Continued on page six)

Reading Privacy Journal's Mail – Airplane Security and Dignity

From Richard Sobel, Northwestern University, Evanston, Ill.: PRIVACY JOURNAL's highlighting two articles in the January issue criticizing the deficiencies of whole-body scanners for air security underscores the failing of the proposed technological fixes and how privacy-respecting approaches can provide more effective results. "Think Twice" underscores how "nude body scanners" "assault . . . the essential dignity of passengers" and likely couldn't find liquid explosives or other explosives cleverly hidden on or in someone's body. Their huge cumulative costs waste resources better targeted on traditional police work of thwarting threats before they get to airports.

"How to Protect Airplanes" identifies technological approaches at airports and onboard that can detect chemical signatures in privacy-respecting ways. More invasive technologies and ID requirements, instead, obscure ways to stop threats earlier and to detect actual dangers.

The controversial issues of dogs and drugs shouldn't distract from the need to combine effective technologies discreetly with privacy- and dignity-respecting security procedures. Related critiques and my edited version appear at www.cyberprivacproject.org.

To correct an error, the ticket [purchased by the identified Amsterdam-Detroit terrorist] was roundtrip, not one-way.

From Darrell Evans, Executive Director, British Columbia Freedom of Information and Privacy Association, Vancouver, B.C., Canada: Tom Riley has retired [see PJ Jan 10], and I would like to write in praise of one of the world's most significant contributors to freedom of information ideals and legislation. The B.C. Freedom of Information and Privacy Association would not exist without Tom, who flew to Vancouver at his own expense in 1990 to help start the organization. Tom was directly involved in planning both the type of legislation we would aim for and the strategy for achieving it. He advised constantly for two years. Two years later, Tom did all the same work in Alberta as the successful movement to get its FOIPP act passed began there. And for at least 20 years, Tom did much the same thing around the world in places like Hong Kong and Eastern Europe as FOI came into focus there as a democratic goal.

From Ann Cavoukian, Information and Privacy Commissioner, Ontario: Tom Riley has had a strong presence in the areas of access and privacy for many years – greatly advancing interest in both fields.

From the Australian Capital Territory, Australia: You must have produced even more [privacy materials] than others over the years. I suspect that might make you the world's largest producer of works on privacy.

Not the Same as Bystanders

We run the risk, each time we leave home and enter public spaces, that we will be observed by strangers. That does not mean that we consent to a permanent video record of our comings and goings. Here's how TV surveillance in public places differs from human observation:

Does not rely on the limits of human memory and eyesight.

Can be searched electronically, by time, place, or biometric characteristics.

Is impersonal and degrading. Intimidating because of its breadth and round-the-clock attributes.

Need not be labor intensive. Images may be stored endlessly and distributed freely.

Has monetary value, unlike human observation.

Can be focused on certain ethnic groups.

Can view through darkness, zoom in and swivel.

Quotable

"Google thrives where privacy does not.''

- Chirag Patnaik, otherwise known as blogger Marlinspike.

Signs That Attitudes on Camera Surveillance Shifting

Great Britain is experiencing TV surveillance fatigue, says a young scholar who has studied the inner workings of cameras (CCTV) in England.

"We may be seeing a diminution," said Gavin J.D. Smith, a lecturer in sociology at City University in London who spent long hours with the operators and observers of the cameras and wrote his PhD thesis on the effects of the operation on observers, not the observed. One operator told him, "It's over. TV surveillance is dead." Smith's findings? "It's a screwed-up work culture," bringing to mind William Faulkner's recurrent literary theme that victimizers often become victims and oppressors experience more mental anguish than the oppressed.

Smith predicted that within ten years the cameras in England, which appears to be the world's most monitored society (about one public camera for each 14 citizens), would be dismantled. (In a keynote address, Clive Norris, a sociologist at the University of Sheffield and one of the most prominent critics of TV surveillance in England, mentioned that Chicago may be supplanting London as the world's most monitored city.)

The news media have turned against the idea, Smith and other scholars reported at a research workshop on camera surveillance at Queen's University in Kingston, Ontario, Canada, last month. The press used to trumpet cameras as a magic solution after "signal events" like a notorious child kidnapping-murder in England in 1993 or the World Trade Center attack in 2001. Perhaps "signal privacy invasions" would cause a shift in public opinion about cameras, suggested sociologist Aaron Doyle of Carleton University in Ottawa. Now news reports refer to "spy cameras," publish headlines like CAMERAS FAIL TO SOLVE CRIMES, and question the use of public expenditures on unproven cameras in public.

Discontinuations in Canada

Emily Smith, of the Surveillance Studies Centre at Queen's, reported that in Canada "there are many examples of camera systems being discontinued or dismantled." She gave as examples Sherbrooke in Quebec, Vancouver in British Columbia, and Brockville in Ontario. In addition, Montreal and Edmonton found the cameras marginally effective. Critics have cited damaged equipment, labor disruptions, an absence of maintenance, targeting of racial minorities (in Canada and the United Kingdom), tight budgets, invasion of privacy, and an inability to monitor the millions of images as reasons for abandoning public TV surveillance.

More and more, in Great Britain and Canada, TV cameras mounted on police cars are equipped with automatic license-plate recognition, allowing authorities to match numbers with autos registered to criminal suspects.

Although Clive Norris called the operation in England "a fiasco," he said that "the narrative is still one of success" and that elected officials voting against cameras after a notable crime will be voted out of office. While "trigger events" still prompt installation of cameras, he said, it is now still obligatory that any new construction

PRIVACY JOURNAL

Founded in 1974

Robert Ellis Smith
Publisher

401/274-7861 fax 401/274-4747

orders@privacyjournal.net

www.privacyjournal.net

PRIVACY JOURNAL is published monthly, reporting on legislation, legal trends, new technology, and public attitudes affecting the confidentiality of personal information. **$125 a year, $165 overseas**. **PRIVACY JOURNAL** is available by postal mail, or by electronic mail, or in selected news and bookstores in the U.S. Back issues are available by mail in hard copy or in electronic form, by email, or at our Web site. MasterCard, Visa, American Express, and Discover credit cards are accepted for payment. **CIRCULATION MANAGER:** Lee Shoreham. **CONTRIBUTING EDITOR:** Marc Osgoode Smith.

20 MINUTES A MONTH

This regular feature provides ways to use 20 minutes of your life each month to protect your privacy or that of others.

Be informed: The census form to be circulated in April has ten questions: number of persons living in the structure; additional persons "staying there"; type of residence and type of financing; telephone number; and the gender, age, date of birth, ethnicity, race, and alternative residence of each person in the household. The Census form does ***not*** require Social Security numbers, salary, credit-card or banking information, marital information, or sexual identity.

Census workers will carry government ID badges and will not ask to enter the house, according to Michael Sean Perry of **PRIVACY JOURNAL**.

Federal law provides a fine of $100 for failure to answer and $500 for answering untruthfully. But this is rarely enforced and courts have not been clear that answering the Census is required.

Personal data held by the Bureau of Census is confidential by law, with stiff penalties for violations, and the bureau has a longtime reputation for vigorously protecting data in its possession.

include untested high-tech security. Vendors of equipment persuade elected officials of the effectiveness of their products without proof. The two-day workshop was held in conjunction with a symposium and art exhibit showcasing artistic creations depicting surveillance regimes. One artist, Dave Kemp of Toronto, collected photos of driver's licenses, student cards, gym memberships, bank cards, credit cards, and other IDs from 85 Canadians and displayed them in a 25-feet wide installation showing how many government and commercial identity cards each person carries – 885 in all – and which documents were "withheld" by the individuals. Manu Luksch of London, England, presented a 50-minute documentary film composed entirely of TV surveillance videotapes acquired under the open-records law in Great Britain. The exhibit continues until April 18 in Kingston, Ontario. www.aeac.ca.

IBM Patents (Continued from page one)

ly mentions license plate recognition technology, face recognition software, and retina scanners. Data captured from video streams from airport cameras is also analyzed," according to Wolfe's report. How can the system analyze all this data and provide a suspicion to airport security personnel in real time? "Computers aren't fast enough to do real-time modeling unless the paradigm shifts," Angell told ***InformationWeek***. "That's why this inference engine is a pretty big deal."

That shift is embedded in how the inference engine is formulated. It uses rule sets, designed by Angell, Friedlander, and Kraemer, which enable it to fairly efficiently query five to ten million data cohorts, in a very short period of time.

New B.C. Commissioner

David Loukidelis, who served as information and privacy commissioner for the Canadian province of British Columbia since 1999, has been appointed deputy attorney general in the provincial government. Paul Fraser, former conflict of interest commissioner, will assume the privacy commissioner role until a permanent replacement is appointed when the legislature reconvenes in the spring.

In a Flash, Online Users Learn of Another Trick on Them

Most personal computer users are now familiar with cookies although that was not true in the early years of the World Wide Web. They know how to delete them if they wish. (Cookies are tiny bits of code injected into the computer of a person browsing the Web, in part to keep track of identifying information, favorite pages, and shopping-cart choices. They also allow Web advertisers to target ads based on PC users' patterns.)

But more than half of the top Web sites insert cookies into Adobe's Flash Player, software used to animate and run video on the Web. "Unlike traditional browser cookies, Flash cookies are relatively unknown to Web users, and they are not controlled through the cookie privacy controls in a browser. That means even if a user thinks they have cleared their computer of tracking objects, they most likely have not," according to Ryan Singel of ***Wired*** magazine.

Adobe, the manufacturer of Flash Player, admits the safe haven for cookies but prefers the term "local storage capabilities."

Even the White House Web site has at least one Flash cookie.

They Keep Coming Back

"Several services even use the surreptitious data storage to reinstate traditional cookies that a user deleted, which is called 're-spawning' in homage to video games where zombies come back to life even after being 'killed,'" wrote Singel reporting on a University of California Berkeley discovery last summer. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

"So even if a user gets rid of a Web site's tracking cookie, that cookie's unique ID will be assigned back to a new cookie again using the Flash data as the 'backup.'"

FTC Knows Now

Now the Federal Trade Commission knows all about the surreptitious cookies, because the UC team told FTC staff members and a commissioner about them at a roundtable held at Berkeley last month to educate the FTC on changes to its privacy enforcement strategy.

Federal Trade Commission consumer protection head David Vladeck, at the event, warned that the commission is getting ready to go after ad companies that try to evade online consumers' decisions on targets ads. "We are currently examining practices that undermine the tools that consumers can use to opt out of behavioral advertising," Vladeck said. "We hope to announce law enforcement actions later this year," he added, without saying whether he was referring to Flash cookies or not.

Adobe said after the roundtable revelation, "The use of Adobe Flash Player has been instrumental in innovating and forming the Web as we know it today. While the vast majority of Web sites and developers use 'local storage capabilities' (often incorrectly referred to as 'Flash cookies') to provide a better user experience, local storage is sometimes misused by certain Web site operators or ad networks. Adobe proactively encourages our customers to use all Adobe products in responsible, ethical ways. Adobe does not support the use of our products in ways that intentionally ignore the user's expressed intentions."

To learn the Flash cookies in your computer, enter "adobe flash cookies delete" or similar language in a search engine and find your way to Adobe's settings manager. You can delete Flash cookies from individual sites or all at once.

In an effort to ward off FTC regulation, one industry privacy group introduced an icon, a little "i" on an aqua background to alert Web buyers that a site uses demographics and behavioral data in its marketing. Jules Polonetsky, founder of the Future of Privacy Forum, which helped create the symbol, compared it to the familiar triangle made up of three arrows that tells consumers that an item is recyclable.

The Largest Breach

Heartland Payment Systems, the major Princeton, N.J.-based provider of credit and debit-card processing services, has agreed to settle with credit-card companies affected by what may be the largest breach of personal financial data ever – American Express ($3.6 million) and Visa ($60 million). But representatives of banks and credit unions affected by the 2008 breach say Heartland's settlement offer for expenses incurred when tens of millions of credit-card identities were stolen amounts to mere pennies on the dollar. They are balking at accepting it. Five financial institutions have sued to stop the settlement and to assess damages on two banks that acquired Heartland.

Albert Gonzalez, 28, who began his computer-crime carrier as a Miami high school student, pleaded guilty to hacking the Heartland system (a conspiracy that also stole data from Seven-11, Target, J.C. Penney, and Hannaford Brothers stores). The same man last September admitted pulling off what was then the largest breach of financial records, at TJX Companies (T.J. Maxx, Marshalls, HomeGoods, and A.J. Wright in the U.S.; Winners, HomeSense and STYLE SENSE in Canada; and T.K. Maxx and Home Sense in Europe). Gonzalez faces up to 17 or 25 years in prison. A co-conspirator, former Morgan Stanley software engineer Stephen Watt, was sentenced to two years in prison for developing the software to make possible the electronic heist.

Nude Scanners (Continued from page one)

how the images released as samples by the government can easily be "painted" by inverting colors to show intimate body parts (http://bit.ly/4tSGzt). Homeland Security officials also claimed that they contemplate no storage or transmission of the body images off-site, but the Electronic Privacy Information Center (EPIC) showed that documents provided to it under the Freedom of Information Act required manufacturers to provide storing, copying and transmitting capability in the devices.

The American Association for Nude Recreation, the oldest and largest group representing nudists in the U.S. and Canada, has endorsed the use of the backscatter scanners, saying, "If travelers just think of the screen as a virtual skinny-dip, something regarded as American as apple pie since before Norman Rockwell, everyone wins in the name of better air travel security." Many members of the AANR and other nudist groups said immediately that the group must be kidding, or kidding itself.

After the Obama Administration unveiled its proposed budget for Fiscal 2011, EPIC President Marc Rotenberg remarked, "It is disheartening to see the significant increase in spending for [surveillance] programs even as support for basic science is being frozen or cut. Body scanners turn out to be one of the boondoggle projects."

"All they are doing with these expenditures," said Ralph Nader, "is making more terrorists."

Facebook Faces New Canadian Probe

The Privacy Commissioner of Canada has announced a new investigation into Facebook because "some Facebook users are disappointed by certain changes being made to the site, changes that were supposed to strengthen their privacy and the protection of their personal information," in the words of assistant commissioner Elizabeth Denham.

A comprehensive investigation last year [see PJ Aug. 09] cleared Facebook of most privacy complaints except for its indefinite retention of data on members who deactivate their accounts. In mid-December, Facebook revised its privacy settings and required all of its 350 million active members to review their settings. A Canadian resident complained that this resulted in less privacy protection than before.

In the U.S., the Electronic Privacy Information Center filed a similar complaint with the Federal Trade Commission, accusing the social-networking site of "unfair and deceptive business practices." The FTC should require Facebook to return to its pre-December privacy settings, allowing users to control disclosure of personal information and to fully opt out of revealing information to third-parties.

In the States – RFID, Prints

For the third time in the past four years, the House of Representatives in New Hampshire passed legislation to require businesses to notify consumers when items have imbedded RFID tags and to provide restrictions for how those tags are used. It also mandates that a business disable RFID (radio-frequency identification) tags on any purchased item if so demanded by a

consumer. In 2006, the same chamber passed a bill similar to this year's (HB 478 passed Jan. 6). But the Senate gutted the proposal and approved only a provision to create an RFID study commission. That law was enacted. In its 2008 report, the commission shied away from recommending state regulations, including the elements in the legislation passed by the House last month. * * * The New Hampshire House also passed a bill that aims to ban fingerprinting as a "reasonable" mode of identification. The bill follows criticism of a Bank of America policy that requires non-customers to provide fingerprint identification when cashing a check. The new bill, HB 299, would amend an existing state law that lays out acceptable required forms of identification. The bill will next come before the Senate. Meanwhile, Bank of America has voluntarily agreed to stop its fingerprinting in New Hampshire.

In the Courts – Street View

The U.S. Court of Appeals for the Third Circuit has kept alive a western Pennsylvania couple's lawsuit objecting to Google's Street View, but just barely. The appeals court agreed with a trial court that the couple's privacy claims (the "right to publicity" or misappropriation and intrusion upon solitude) were insufficient to take to trial, but that the trial court should hear their claim that Google's camera truck on their premises without consent may constitute a trespass. But under Pennsylvania law, winning a trespass lawsuit may bring only nominal damages and "whatever sense of vindication that may bring." ***Boring v. Google***, 09-2350 (Jan. 25).

□ Customs and Border Protection agents searched more than 1500 laptops and other electronic devices at the U.S. border over nine months prior to June 2009, according to documents obtained by the American Civil Liberties Union in a Freedom of Information Act lawsuit. Customs forwarded electronic files taken from travelers' personal devices nearly 300 times. In a practice begun by the Bush Administration and continued by the Obama government, travelers crossing borders have been reluctant to carry medical records, financial information, and photos when they travel because of fear that U.S. border agents will inspect for no good reason or suspicion of wrongdoing. ***ACLU v. U.S. Department of Homeland Security,*** 09 Civ. 7465 (S.D. N.Y. Aug. 26, 2009).

□ An appeals court in California says an Orange County family may proceed with a lawsuit against the California Highway Patrol, whose employees casually emailed graphic photos of its 19-year-old daughter decapitated after an auto accident – for Halloween shock value. The images have been widely circulated on the Internet. ***Catsouras v. Department of the California Highway Patrol,*** *G039916, G0 40330* (Cal Apps, Feb. 1).

□ Associate Justice Clarence Thomas of the U.S. Supreme Court not only endorsed the court's insistence that governmental limits on corporate political donation are unconstitutional, he also in a separate opinion advocated total secrecy in campaign contributions. That was something his conservative colleagues would not do. Thomas blamed gay opponents of Proposition 8 in California in 2008. He wrote that any individual who contributed as little as $100 in favor of the ban on same-sex marriage was required to disclose his or her name and address to the public, and thus opened themselves up to harassment, "property damage, or threats of physical violence or death, as a result."***Citizens United v. FCC***, 08-205, Jan. 21.

Thomas has elevated the notion of gay-rights groups harassing electoral opponents to the level of conventional wisdom at the Supreme Court, as evidenced by two decisions just prior to the campaign-finance decision. The high court agreed to decide whether the Secretary of State in Washington State may release the names, addresses, and other personal information of more than 138,000 individuals who signed a petition seeking to protect traditional marriage. ***Doe v. Reed***, 09-559 (Jan. 15). Also, in an extraordinary order that echoed Thomas' language in the campaign-finance case, the 5-4 right-wing bloc on the court ordered a federal court in California to halt the televising of a trial currently being conducted on the validity of the original Prop 8 in 2008. ***Hollingsworth v. Perry,*** 09A648 (Jan. 13).

Just Published – Social Nets

Twenty-somethings ***do*** care about privacy on social networking sites; they simply define it

slightly differently and use tricks to circumvent Facebook's disclosure practices, according to "Alias, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook" by Kate Raynes-Goldie, PhD candidate in Internet studies at Curtin University of Technology in Australia. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432.

□ In the Canadian province of Ontario, where patient information gets lost regularly, a nurse for a regional health unit lost a USB stick containing files on 83,524 persons using the clinic. This happened last Dec. 21. This led to a report (HO-007) from the provincial Information and Privacy Commissioner reiterating an order that any patient data in portable devices be encrypted, and immediately. Passwords alone are not adequate protection. To reinforce the message the commissioner included a list of five available encryption products. www.ipc.on.ca.

□ Mere fines do not deter abusive business practices that violate privacy rules, says Information Commissioner in the United Kingdom Christopher Graham. He argues that the maximum penalty of two years' jail time should be the standard for sentences handed out after individuals breach confidentiality. "In many cases a fine alone will be looked on by the offender as little more than a business expense or simply as a risk worth taking" (***ComputerworldUK***, Nov. 27, 2009).

Agenda – Forgetfulness?

A panel discussion as part of the annual Conference on Computers, Privacy and Data Protection in Brussels Jan 29-30 considered an issue now emerging in Europe: "The panel will review forgetfulness from a multidisciplinary perspective and address issues such as the possibility or impossibility of providing new technical, legal or social solutions to better protect forgetfulness (or to allow subjects to regain some control on their personal data). Forgetfulness, or the right to be forgotten, is often referred to as one of the essential dimensions of privacy. Forgetfulness is explicitly protected by privacy laws which require that data must not be recorded longer than the time needed for the purpose of the collection. This principle, however, is very difficult to put into practice at a time when storing information is so cheap and easy that it becomes the by-default rule and data is more and more disseminated over the Internet, creating a new form of nuisance which has been referred to as 'data pollution.'"

□ The verdict on four Google executives on trial in Milan has been postponed to Feb 24 because of an unrelated three-day strike by prosecutors. The four are charged with permitting demeaning images on Google-owned YouTube of an Italian school boy with Down syndrome.

□ ***Social Research***, the international quarterly of The New School for Social Research, will host a public conference on "Limiting Knowledge in a Democracy" Feb. 24-26, 2010, in New York City and will subsequently publish the conference proceedings as an issue of the journal. Information from Roberta Sutton, 212/ 229-5776, ext. 3121, socres@newschool.edu, www.socres.org/limiting knowledge.

□ Cloud computing and behavioral tracking will be discussed at the Consumer Federation of America's Consumer Assembly, which has been held since 1967. It begins Mar 11 in Washington, D.C., and ends Mar. 12. Information from Sally Karwowski, 202/939-1005, skarwowski@consumerfed.org.

□ The third and final Federal Trade Commission roundtable on its re-evaluation of its compliance program will take place Mar. 17 in Washington. Information from privacyround@ftc.gov, www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml#participate.

□ Librarians at the University of Rhode Island will hold a forum Mar. 31, as a prelude to a new initiative by librarians called "Choose Privacy Week" the first week in May. www.privacyrevolution.org/index.php/privacy_week/. Publisher Robert Ellis Smith will participate at URI. Information from Jim Kinnie, jkinnie@mail.uri.edu.

□ The fourth biannual conference on Surveillance and Society will be held April 13-15 at City University London, thought to be the only university in the world offering a master's degree in surveillance studies. The sponsor is European Cooperation in Science and Technology (COST) Action. Topics include the development of and the business of surveillance technology; public attitudes, policies, and the economics of surveillance. Information at www.city.ac.uk/sociology/Department_News/ews.html, surveillance_conference@live.co.uk.