

Technology Issues Report April 2006

1/ **Border Security System Left Open.** A computer failure that hobbled border-screening systems at airports across the country last August occurred after Homeland Security officials deliberately held back a security patch that would have protected the sensitive computers from a virus then sweeping the Internet, according to documents obtained by Wired News. The documents raise new questions about the \$400 million US-VISIT program, a 2-year-old system aimed at securing the border from terrorists by gathering biometric information from visiting foreign nationals and comparing it against government watch lists.

The Aug. 18 computer failure led to long lines at international airports in Los Angeles, San Francisco, Miami and elsewhere, while U.S. Customs and Border Protection, or CBP, officials processed foreign visitors by hand, or in some cases used backup computers, according to contemporaneous press reports. Publicly, officials initially attributed the failure to a virus, but later reversed themselves and claimed the incident was a routine system failure.

US-VISIT consists of a hodgepodge of older mainframe databases, fronted by Windows 2000 workstations installed at nearly 300 airports, seaports and border crossings around the country. Government investigators have found the mainframes pretty secure, but confirm that security holes are present on the PC end of the system.

CBP officials have released six pages of heavily redacted documents about the Aug. 18 computer failure. But two CBP reports obtained under the Freedom of Information Act show that the virulent Zotob internet worm infiltrated agency computers the day of the outage, prompting a hurried effort to patch hundreds of Windows-based US-VISIT workstations installed at nearly 300 airports, seaports and land border crossings around the country.

"When the virus problems appeared on (CBP) workstations Thursday evening, the decision was made to push the patch, immediately, to the ... US-VISIT workstations. Most workstations had received the patch by midnight and US-VISIT was back in operation at all locations," reads a CBP summary of the incident. The Department of Homeland Security's US-VISIT program office declined to comment on the documents.

Former White House cybersecurity adviser Howard Schmidt says the incident is typical of a large agency struggling with complex networks and evolving threats. "We've got catching-up to do in all areas, particularly areas having to do with national security and public safety," says Schmidt. "I hope you and I, 10 years from now, look back and say, 'Wow, I'm glad we survived that.'"

Launched in January 2004, and expanded since then, US-VISIT is a hodgepodge of older databases maintained by various government agencies, tied to a national CBP-run network of Windows 2000 Professional workstations installed at U.S. points of entry. The system has processed more than 52 million visitors, and allowed border officials to intercept more than 1,000 wanted criminals and immigration violators, according to DHS. Some US-VISIT locations are now testing gear to read new RFID-equipped passports.

While the idea of US-VISIT is universally lauded within government, the program's implementation has faced a steady barrage of criticism from congressional auditors concerned over management issues and cybersecurity problems. Last December, the DHS inspector general reported that the program might be vulnerable to hackers.

The nearly 6-year-old Windows 2000 operating system was a particularly burdensome choice on Aug. 9, when Microsoft announced a vulnerability in the software's plug-and-play feature that allowed attackers to take complete control of a computer over a network. In an unusually quick mating of vulnerability with attack, it took only four days for a virus writer to launch an Internet worm, called Zotob that spread through the security hole. Operating somewhat more slowly, it took CBP officials until Aug. 16 -- a full week after Microsoft released a patch for the hole -- to start pushing the fix to CBP's Windows 2000 computers. But because of the array of peripherals hanging off of the US-VISIT workstations -- fingerprint readers, digital cameras and passport scanners -- they held off longer on fixing those machines, for fear that the patch itself might cause a disruption.

"The push was not made to the US-VISIT workstations during the initial install due to concerns with the possible impact of the patch on the unique workstation configurations," reads one of the CBP reports.

Officials -- not unreasonably, say security experts -- wanted to test the patch before installing it. But as a consequence, hundreds of computers networked to sensitive law enforcement and intelligence databases were left with a known vulnerability -- a security hole rated "critical" by Microsoft because it allows attackers to take control of a machine remotely. It wasn't until Zotob made itself at home on the CBP network Aug. 18 that the agency launched a fevered effort to secure the US-VISIT terminals, which sit on local area networks that are in turn connected to CBP's wide area network. Even as officials raced to install the patches, the US-VISIT computers were failing at major U.S. entry points around the country, including airports in Dallas, Houston, Los Angeles, Miami, New York, San Francisco and Laredo, Texas, according to press reports at the time.

A DHS spokesman told the Associated Press the next day that a virus caused the outages. But in December, a different DHS spokesman told CNET News.com that there was no evidence that a virus was responsible, and that it was merely one of the routine "computer glitches" one expects in any complex system. The newly released documents call that claim into question.

The government did not part with the pages lightly. After an initial FOIA request was rebuffed, Wired News filed a federal lawsuit, represented by Megan Adams, a law student at the Stanford Law School Cyberlaw Clinic. Only then did CBP release six pages of heavily redacted documents, including one page that is completely blacked out. (The lawsuit is ongoing.) The redactions leave it unclear whether the virus itself shuttered the system, or whether the patch, or the process of installing it, contributed to the outage. For example, one sentence reads, "Initial reports confirmed that the US-VISIT workstations were (redacted) impacted" by the virus. The blacked-out portion might as easily read "severely" as "not." Other redactions appear less tactical:

A public Microsoft security bulletin is included, but with the bulletin number (MS05-039) blacked out.

Perhaps most significantly, the pages do not reveal how the Zotob virus made its way onto the private CBP network -- an ominous migration that demonstrates that computers used in protecting U.S. borders are accessible, via some path, from the public Internet, and could be subject to tampering. "That machine was reachable from some network, that was connected to some other network, that was connected to the Internet," says Tim Mullen, a Windows security expert and CIO of security firm AnchorIS. "There was some series of connections that manifested itself in those machines getting compromised."

A September report by the DHS inspector general found computer security at CBP wanting. In a scan of 368 devices on CBP networks, investigators identified 906 security vulnerabilities rated as medium or high risk. They criticized CBP for failing to implement a comprehensive security-testing program, among other issues. "Our vulnerability assessments identified security concerns resulting from inadequate password controls, missing critical patches, vulnerable network devices and weaknesses in configuration management," the report concludes. "These security concerns provide increased potential for unauthorized access to CBP resources and data."

In a second report in December focused on US-VISIT, the inspector general concluded that the mainframe databases at the backend of the system were generally secure. But investigators found vulnerabilities elsewhere in the system's architecture that "could compromise the confidentiality, integrity and availability of sensitive US-VISIT data." In particular, the report found system vulnerabilities at the U.S. points of entry where the US-VISIT workstations are operating. It blames the weaknesses on poor communications between administrators in the field and those at US-VISIT's Virginia data centre. In February, the Government Accountability Office -- Congress' investigative arm -- followed up with its own investigation of the program, faulting US-VISIT for not having an overall security plan.

Besides management issues, the system has been criticized as a slapdash effort at stringing older technology together into a modern security screening system. "Biometrics have been introduced into an antiquated computer environment," the 9/11 Commission noted of the program. "Replacement of these systems and improved biometric systems will be required."

Schmidt agrees, though he says the problem is hardly limited to US-VISIT. "We have to start moving at industry speed, not government speed, when it comes to the deployment of new technologies," says Schmidt. Instead of running Windows 2000, "I'd be racing to run the beta of the next generation of operating system ... and not worry about legacy stuff that we know isn't going to be supported too much longer and has had issues."

Prior to infecting CBP, the Zotob virus reportedly caused disruptions at The New York Times, ABC and CNN's headquarters in Atlanta, as well as some offices on Capitol Hill. In late August, the FBI announced the arrest of two men in connection

with the worm: 18-year-old Farid "Diabl0" Essebar in Morocco, and a 21-year-old Turkish man named Atilla Ekici, known online as "Coder." (Wired News 12/4/06)

2/ **The Anti-ID-Theft Bill That Isn't.** Security Matters. California was the first state to pass a law requiring companies that keep personal data to disclose when that data is lost or stolen. Since then, many states have followed suit. Now Congress is debating federal legislation that would do the same thing nationwide. Except that it won't do the same thing: The federal bill has become so watered down that it won't be very effective. I would still be in favour of it -- a poor federal law is better than none - - if it didn't also pre-empt more-effective state laws, which makes it a net loss.

Identity theft is the fastest-growing area of crime. It's badly named -- your identity is the one thing that cannot be stolen -- and is better thought of as fraud by impersonation. A criminal collects enough personal information about you to be able to impersonate you to banks, credit card companies, brokerage houses, etc. Posing as you, he steals your money, or takes a destructive joyride on your good credit. Many companies keep large databases of personal data that is useful to these fraudsters. But because the companies don't shoulder the cost of the fraud, they're not economically motivated to secure those databases very well. In fact, if your personal data is stolen from their databases, they would much rather not even tell you: Why deal with the bad publicity?

Disclosure laws force companies to make these security breaches public. This is a good idea for three reasons.

One, it is good security practice to notify potential identity theft victims that their personal information has been lost or stolen.

Two, statistics on actual data thefts are valuable for research purposes.

And three, the potential cost of the notification and the associated bad publicity naturally leads companies to spend more money on protecting personal information -- or to refrain from collecting it in the first place. Think of it as public shaming. Companies will spend money to avoid the PR costs of this shaming, and security will improve. In economic terms, the law reduces the externalities and forces companies to deal with the true costs of these data breaches.

This public shaming needs the cooperation of the press and, unfortunately, there's an attenuation effect going on. The first major breach after California passed its disclosure law -- SB1386 -- was in February 2005, when ChoicePoint sold personal data on 145,000 people to criminals. The event was all over the news, and ChoicePoint was shamed into improving its security. Then LexisNexis exposed personal data on 300,000 individuals. And Citigroup lost data on 3.9 million individuals. SB1386 worked; I believe the only reason we knew about these security breaches was because of the law. But the breaches came in increasing numbers, and in larger quantities. After a while, it was no longer news. And when the press stopped reporting, the "cost" of these breaches to the companies declined.

Today, the only real cost that remains is the cost of notifying customers and issuing cards. It costs banks about \$10 to issue a new card, and that's money they would much

rather not have to spend. This is the agenda they brought to the federal bill, cleverly titled the Data Accountability and Trust Act, or DATA.

Lobbyists attacked the legislation in two ways. First, they went after the definition of personal information. Only the exposure of very specific information requires disclosure. For example, the theft of a database that contained people's first initial, middle name, last name, Social Security number, bank account number, address, phone number, date of birth, mother's maiden name and password would not have to be disclosed, because "personal information" is defined as "an individual's first and last name in combination with..." certain other personal data.¹

Second, lobbyists went after the definition of "breach of security." The latest version of the bill reads: "The term 'breach of security' means the unauthorized acquisition of data in electronic form containing personal information that establishes a reasonable basis to conclude that there is a significant risk of identity theft to the individuals to whom the personal information relates." Get that? If a company loses a backup tape containing millions of individuals' personal information, it doesn't have to disclose if it believes there is no "significant risk of identity theft." If it leaves a database exposed, and has absolutely no audit logs of who accessed that database, it could claim it has no "reasonable basis" to conclude there is a significant risk. Actually, the company could probably point to a study that showed the probability of fraud to someone who has been the victim of this kind of data loss to be less than 1 in 1,000 -- which is not a "significant risk" -- and then not disclose the data breach at all.

Even worse, this federal law pre-empts the 23 existing state laws -- and others being considered -- many of which contain stronger individual protections. So while DATA might look like a law protecting consumers nationwide, it is actually a law protecting companies with large databases from state laws protecting consumers.

So in its current form, this legislation would make things worse, not better. Of course, things are in flux. They're always in flux. The language of the bill has changed regularly over the past year, as various committees got their hands on it. There's also another bill, HR3997, which is even worse. And even if something passes, it has to be reconciled with whatever the Senate passes, and then voted on again. So no one really knows what the final language will look like. But the devil is in the details, and the only way to protect us from lobbyists tinkering with the details is to ensure that the federal bill does not pre-empt any state bills: that the federal law is a minimum, but that states can require more.

That said, disclosure is important, but it's not going to solve identity theft. As I've written previously, the reason theft of personal information is so common is that the data is so valuable. The way to mitigate the risk of fraud due to impersonation is not to make personal information harder to steal, it's to make it harder to use.

Disclosure laws only deal with the economic externality of data brokers protecting your personal information. What we really need are laws prohibiting credit card companies and other financial institutions from granting credit to someone using your name with only a minimum of authentication. But until that happens, we can at least hope that Congress will refrain from passing bad bills that override good state laws -- and helping criminals in the process. (Wired News 20/4/06)

3/ **Whistle-Blower Outs NSA Spy Room.** AT&T provided National Security Agency eavesdroppers with full access to its customers' phone calls, and shunted its customers' Internet traffic to data-mining equipment installed in a secret room in its San Francisco switching centre, according to a former AT&T worker cooperating in the Electronic Frontier Foundation's lawsuit against the company.

Mark Klein, a retired AT&T communications technician, submitted an affidavit in support of the EFF's lawsuit this week. That class action lawsuit, filed in federal court in San Francisco last January, alleges that AT&T violated federal and state laws by surreptitiously allowing the government to monitor phone and Internet communications of AT&T customers without warrants. On Wednesday, the EFF asked the court to issue an injunction prohibiting AT&T from continuing the alleged wiretapping, and filed a number of documents under seal, including three AT&T documents that purportedly explain how the wiretapping system works.

According to a statement released by Klein's attorney, an NSA agent showed up at the San Francisco switching centre in 2002 to interview a management-level technician for a special job. In January 2003, Klein observed a new room being built adjacent to the room housing AT&T's #4ESS switching equipment, which is responsible for routing long distance and international calls. "I learned that the person whom the NSA interviewed for the secret job was the person working to install equipment in this room," Klein wrote. "The regular technician work force was not allowed in the room."

Klein's job eventually included connecting Internet circuits to a splitting cabinet that led to the secret room. During the course of that work, he learned from a co-worker that similar cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego. "While doing my job, I learned that fiber optic cables from the secret room were tapping into the Worldnet (AT&T's internet service) circuits by splitting off a portion of the light signal," Klein wrote. The split circuits included traffic from peering links connecting to other internet backbone providers, meaning that AT&T was also diverting traffic routed from its network to or from other domestic and international providers, according to Klein's statement.

The secret room also included data-mining equipment called a Narus STA 6400, "known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for preprogrammed targets," according to Klein's statement. Narus, whose website touts AT&T as a client, sells software to help internet service providers and telecoms monitor and manage their networks, look for intrusions, and wiretap phone calls as mandated by federal law.

Klein said he came forward because he does not believe that the Bush administration is being truthful about the extent of its extrajudicial monitoring of Americans' communications. "Despite what we are hearing, and considering the public track record of this administration, I simply do not believe their claims that the NSA's spying program is really limited to foreign communications or is otherwise consistent with the NSA's charter or with FISA," Klein's wrote. "And unlike the controversy over targeted wiretaps of individuals' phone calls, this potential spying appears to be applied wholesale to all sorts of Internet communications of countless citizens."

After asking for a preview copy of the documents last week, the government did not object to the EFF filing the paper under seal, although the EFF asked the court Wednesday to make the documents public. One of the documents is titled "Study Group 3, LGX/Splitter Wiring, San Francisco," and is dated 2002. The others are allegedly a design document instructing technicians how to wire up the taps, and a document that describes the equipment installed in the secret room.

In a letter to the EFF, AT&T objected to the filing of the documents in any manner, saying that they contain sensitive trade secrets and could be "could be used to 'hack' into the AT&T network, compromising its integrity." According to court rules, AT&T has until Thursday to file a motion to keep the documents sealed. The government could also step in to the case and request that the documents not be made public, or even that the entire lawsuit be barred under the seldom-used State Secrets Privilege.

AT&T spokesman Walt Sharp declined to comment on the allegations, citing a company policy of not commenting on litigation or matters of national security, but did say that "AT&T follows all laws following requests for assistance from government authorities." (Wired News 7/4/06)

4/ **More on the same as 3/ AT&T Seeks to Hide Spy Docs.** AT&T is seeking the return of technical documents presented in a lawsuit that allegedly detail how the telecom giant helped the government set up a massive internet wiretap operation in its San Francisco facilities.

In papers filed late Monday, AT&T argued that confidential technical documents provided by an ex-AT&T technician to the Electronic Frontier Foundation shouldn't be used as evidence in the case and should be returned. The documents, which the EFF filed under a temporary seal last Wednesday, purportedly detail how AT&T diverts Internet traffic to the National Security Agency via a secret room in San Francisco and allege that such rooms exist in other AT&T switching centres. The EFF filed the class-action lawsuit in U.S. District Court in Northern California in January, seeking damages from AT&T on behalf of AT&T customers for alleged violation of state and federal laws.

Mark Klein, a former technician who worked for AT&T for 22 years, provided three technical documents, totalling 140 pages, to the EFF and to The New York Times, which first reported last December that the Bush administration was eavesdropping on citizens' phone calls without obtaining warrants. Klein issued a detailed public statement last week, saying he came forward because he believes the government's extrajudicial spying extended beyond wiretapping of phone calls between Americans and a party with suspected ties to terrorists, and included wholesale monitoring of the nation's internet communications.

AT&T built a secret room in its San Francisco switching station that funnels Internet traffic data from AT&T Worldnet dialup customers and traffic from AT&T's massive Internet backbone to the NSA, according to a statement from Klein. Klein's duties included connecting new fibre-optic circuits to that room, which housed data-mining equipment built by a company called Narus, according to his statement.

Narus' promotional materials boast that its equipment can scan billions of bits of Internet traffic per second, including analysing the contents of e-mails and e-mail attachments and even allowing playback of Internet phone calls.

While AT&T's open filings did not confirm the details of Klein's statement, they did not dispute the legitimacy of his claims, and the company's filing included a sealed affidavit attesting to the sensitivity of the documents. The company asked for a hearing Thursday to determine whether the documents could be used in the class-action lawsuit, whether they would be unsealed or whether the EFF would have to return them. The EFF filed a rebuttal, calling that time frame unworkable and accusing AT&T of not following normal court rules.

AT&T's lawyers also told the court that intense press coverage surrounding the case, including Wired News' publication of Klein's statement, was revealing the company's trade secrets, "causing grave injury to AT&T." The lawyers argued that unsealing the documents "would cause AT&T great harm and potentially jeopardize AT&T's network, making it vulnerable to hackers, and worse."

The EFF filed the documents last week under a temporary seal when it asked the judge to force AT&T to stop the alleged Internet spying until the case goes to trial. Klein's statement and documents are the only direct evidence filed so far by the EFF, and without them its case could be weakened. It is not clear whether AT&T has served legal papers to Klein.

As of last week, Klein was represented by Miles Ehrlich, who until January served as a U.S. attorney in San Francisco, prosecuting white-collar crime. Klein is now also represented by two lawyers from the powerhouse law firm Morrison & Foerster, including James J. Brosnahan, who is best known for representing John Walker Lindh, the Marin County, California, man found fighting for the Taliban in Afghanistan. The EFF declined to comment on the filing, while AT&T did not return a call seeking comment. The case is *Hepting v. AT&T*. (Wired News 12/4/06):

5/ **Group: Yahoo Helped China, Again.** BEIJING -- Yahoo turned over a draft e-mail from one of its users to Chinese authorities, who used the information to jail the man on subversion charges, according to the verdict from his 2003 trial released Wednesday by a rights group. It was the third time the U.S.-based Internet company has been accused of helping put a Chinese user in prison.

Jiang Lijun, 39, was sentenced to four years in prison in November 2003 for subversive activities aimed at overthrowing the ruling Communist Party. Hong Kong-based Yahoo Holdings Ltd., a unit of Yahoo, gave authorities a draft e-mail that had been saved on Jiang's account, Reporters Without Borders said, citing the verdict by the Beijing No. 2 People's Court. The Paris-based group provided a copy of the verdict, which it said it obtained this week. Yahoo spokeswoman Mary Osako said the Sunnyvale, California-based company is not familiar with Jiang's case. "We condemn punishment of any activity internationally recognized as free expression, whether that activity takes place in China or anywhere else in the world," she said.

The draft e-mail, entitled "Declaration," was similar to manuscripts called "Freedom and Democracy Party Program" and "Declaration of Establishment" that were

recovered from a computer and a floppy disk owned by two other Internet activists, the verdict said.

The information was listed in the verdict under "physical evidence and written evidence." It proved that Jiang and the other activists were planning to "make preparations for organizing a party and to use violence to overthrow the Communist Party," the verdict said. Jiang also was one of five activists who signed an open letter calling for political reform that was posted on the Internet ahead of the Communist Party congress -- a major event -- in November 2002. "Little by little we are piecing together the evidence for what we have long suspected, that Yahoo is implicated in the arrest of most of the people we have been defending," Reporters Without Borders said in a statement. The group said there were other cases that were similar, but it could not release any details because they were still being investigated.

While China encourages use of the Internet for business and education, it also tightly controls web content, censoring anything it considers critical or a threat to the Communist Party. Blogs often are shut down, and users who post articles promoting Western-style democracy and freedom are regularly detained and jailed under vaguely worded subversion charges. Yahoo also has been criticized by rights groups by providing information in the cases of Li Zhi and Shi Tao.

Li, from southwestern China, was sentenced to prison for subversion after posting comments online criticizing official corruption. Shi, a reporter, was sentenced to 10 years in prison after he sent an e-mail abroad containing notes about a government memo on media restrictions. Foreign Ministry spokesman Qin Gang said in February that China has a right to police the Internet and "guide its development in a healthy and orderly fashion."

Google and Microsoft also have been accused of enforcing Chinese censorship guidelines. Google started a Chinese version of its popular search engine that omits links to content deemed unacceptable by the government. Microsoft shut down, at Beijing's request, a popular Chinese blog that touches on sensitive topics such as press freedoms.

American lawmakers have taken the companies to task, accusing them at congressional hearings of helping China crush dissent in return for access to its lucrative and rapidly expanding Internet market. China already has the world's second-largest Internet population, behind the United States, with more than 100 million people online. The Reporters Without Borders report came as Chinese President Hu Jintao visited the United States. His first stop was Seattle, where he dined with Microsoft chairman Bill Gates. (Wired News 19/4/06)

6/ **IBM Touts Integrated Encryption.** In an effort to boost the level of data security on portable computers, cell phones and other gadgets, IBM is unveiling a method for injecting encryption capabilities into the heart of the machines' circuitry. There are multiple ways to achieve encryption, the mathematical art of encoding data to protect it from spying eyes. Specialized software can do the trick, as can hard-wired chips inside computers.

But IBM researchers contend that unless the encryption function is performed by a computer's central processing unit, a supremely savvy hacker can tap into the pathway between the machine's brain and the separate encryption engine. To guard against that, IBM said Monday that it has developed SecureBlue — a set of encryption circuitry that can be integrated into any processor, regardless of its manufacturer. "This thing is trying to be one of the most paranoid devices on the planet," said Charles Palmer, IBM's head security researcher.

IBM is not the first to seek to integrate encryption into a computer's central processing functions. Intel's upcoming LaGrande technology essentially does that, though it requires interaction with a separate chip, known as a trusted platform module.

The IBM researchers say they have developed a way to skip that step. Richard Doherty, an analyst with the Envisioneering Group, said SecureBlue's design appears flexible enough to bring strong encryption to such new settings as cell phones and music players. That could mean enhanced security not only for users who keep sensitive data on portable devices, but also for content owners who can use encryption to lock down copyrighted material and prevent it from being freely disseminated.

However, IBM's encryption engine is not simply a module that can be plugged into existing chips. SecureBlue needs to be woven into a processor from scratch, mixed in with other transistors somewhat "like hamburger," in the description of Bernie Meyerson, chief technologist for IBM's systems group. That means SecureBlue, at least for the time being, likely will end up only in devices made by companies that hire IBM's custom engineering unit. That group's projects include chips for medical and defence systems and video game consoles made by Microsoft, Nintendo and Sony. IBM researchers said SecureBlue already has made its way into one customer's devices. But they said that company had demanded anonymity.

Considering that software vendors such as PGP Corp. already offer software-based encryption for portable devices such as BlackBerrys, IBM might have to convince sceptics that SecureBlue significantly raises the bar for security. Bruce Schneier, founder of Counterpane Internet Security, said more fully integrating encryption and processing would likely improve a machine's performance. But he said it was "just stupid" to claim that hackers would otherwise target the transmission between a computer processor and a separate encryption engine.

Far more likely, he said, is for someone to try to steal data when it was unencrypted — such as when it appeared in plain text on a computer screen. "Security is a chain and it's as strong as its weakest link," he said. "They're talking about taking a very strong link and making it a little bit stronger, at best. Maybe." (Wired News 10/4/06)

7/ **Gates and Hu: Feel the Love.** After a swanky dinner with the world's richest man, Chinese President Hu Jintao turns his attention to America's largest exporter, whose sales to China could help ease tensions over a growing trade gap. Hu, who dined Tuesday night at the home of Microsoft chairman Bill Gates, was invited to tour Boeing's Everett plant on Wednesday, just days after Chinese officials confirmed a commitment to order 80 Boeing 737 jets, in a deal valued at \$5.2 billion

at list prices. The order has yet to be finalized, and airlines typically negotiate discounts.

Boeing sees China as one of its most important future markets, estimating that the country will require 2,600 new airplanes over the next 20 years. The big Boeing deal is one of several purchases the Chinese made recently as officials try to ease tensions over the massive trade gap between the two nations. It's one of several issues President Bush is expected to raise when Hu heads to Washington, D.C., later in his four-day U.S. tour. Hu's Thursday summit with Bush will cover a broad agenda, from China's much-criticized currency and other trade policies, to its aggressive search for oil and its positions on the developing nuclear programs in Iran and North Korea.

Touring Microsoft's suburban Redmond campus earlier Tuesday, Hu said he admired what Gates had achieved. He also sought to reassure Gates that China is serious about protecting intellectual property rights, a key concern for the company as it battles widespread piracy of its Windows operating system there. "Because you, Mr. Bill Gates, are a friend of China, I'm a friend of Microsoft," Hu said through a translator. "Also, I am dealing with the operating system produced by Microsoft every day," he added, to laughter.

Gates responded: "Thank you, it's a fantastic relationship," and then quipped: "And if you ever need advice on how to use Windows, I'll be glad to help."

In a whirlwind visit, Hu — accompanied by Gates, company CEO Steve Ballmer and an entourage of Chinese dignitaries — saw some business technology demonstrations and toured Microsoft's Home of the Future, which features experimental technology.

Hu began his American visit Tuesday in Everett, about 30 miles north of Seattle, where he was greeted by a local kung fu club and a handful of ribbon dancers from a Seattle elementary school. Hu also was greeted by government and business leaders, including Gov. Chris Gregoire and Starbucks chairman Howard Schultz. Hu told Gregoire he didn't choose Seattle simply because it's the closest major U.S. city to China. "It is also because your state enjoys very good cooperative relations with my country," Hu said through a translator. China is Washington state's third-largest export market, while Washington imported more than \$16 billion worth of products from China in 2005.

Demonstrators both in support and opposition to Hu lined the streets near his downtown Seattle hotel. Supporters waved Chinese and American flags. Members of the spiritual movement Falun Gong, condemned by the Chinese government as an evil cult, staked out all four corners around the hotel Tuesday to protest treatment of the movement's followers in China. At the entrance to Microsoft's campus, protesters waved signs in Chinese and English that read "Stop web censorship" and "Release all political prisoners."

Following the meeting at Microsoft, about 100 guests were invited to Gates' home for a dinner Gregoire hosted there. The guest list included executives from Costco, Weyerhaeuser, Boeing and Amazon.com.

The visit came as Microsoft, after years of battling widespread software piracy in the potentially lucrative China market, is hopeful that things are changing. Chinese government officials say they are serious about cracking down on sales of illegal copies of Microsoft's Windows operating system, and some computer makers are pledging to ship more computers with legitimate Windows software installed. Although analysts say it could be some time before the promised changes have a significant effect on Microsoft's sales, the pledges are a feel-good backdrop for Hu's visit with Gates and other business and government executives
(Wired News 19/4/06)

8/ **Anti-terror bill limits FOI.** INCREASED restrictions on freedom of information requests, and 10 years' jail for providing information to assist with terrorist acts, are features of a new Victorian anti-terror bill that entered State Parliament last week. The new laws would also exempt some documents from the existing 30-year limit, allowing the Government to withhold them indefinitely.

Under the legislation it would be an offence to provide documents or information that facilitated a terrorist act, punishable by up to 10 years' jail. Restrictions on freedom of information laws would also be expanded to make it more difficult to obtain information on security issues. Any documents created by the counter-terrorism co-ordination and emergency management department of Victoria Police would be exempt from freedom of information requests. Also exempt would be any documents that endangered the security of premises and those related to risk-management plans and training exercises.

The Terrorism (Community Protection) (Further Amendment) Bill amends the Public Records Act 1973 to allow records to be withheld beyond the 30-year period currently provided under the act. "The bill amends the Public Records Act to deal with security-sensitive documents held by the Public Records Office," Attorney-General Rob Hulls told State Parliament on Thursday. The new law would allow the minister to determine that a document "cease to be, or is not to be, available for public inspection either indefinitely or for the specified period". The new section would also allow the minister to permit access to withheld documents for research purposes on condition researchers did not publish or pass on the relevant document. "Here it is appropriate that an offence is prescribed for any breach of a condition or restriction," Mr Hulls said.

Opposition attorney general Andrew McIntosh said it was important to have an independent body to ensure the Government did not misuse the new restrictions. "I just don't trust (the Government), they will use every avenue possible to get documents exempted from freedom of information, including asking for a clearer definition of what do you mean by the word 'contract'," he said.

A spokeswoman for Mr Hulls, Liz Armitage, said the Victorian Civil and Administrative Appeals Tribunal would be able to rule on any security-related freedom of information requests. "The Terrorism (Community Protection) (Further Amendment) Bill does not affect existing review mechanisms in relation to security risk documents," she said. "VCAT does have power to determine whether there were reasonable grounds for exempting a security risk document from an FOI request." The bill will be debated in State Parliament on May 2. (theage.com.au 9/4/06)

9/ **More on 3 and 4 Wiretap Whistleblower's Statement.** Former AT&T technician Mark Klein has come forward to support the EFF's lawsuit against AT&T for its alleged complicity in the NSA's electronic surveillance. Here, Wired News publishes Klein's public statement in its entirety.

Statement: Mark Klein, April 6, 2006

My background: For 22 and 1/2 years I worked as an AT&T technician, first in New York and then in California.

What I observed first-hand:

In 2002, when I was working in an AT&T office in San Francisco, the site manager told me to expect a visit from a National Security Agency agent, who was to interview a management-level technician for a special job. The agent came, and by chance I met him and directed him to the appropriate people.

In January 2003, I, along with others, toured the AT&T central office on Folsom Street in San Francisco -- actually three floors of an SBC building. There I saw a new room being built adjacent to the 4ESS switch room where the public's phone calls are routed. I learned that the person whom the NSA interviewed for the secret job was the person working to install equipment in this room. The regular technician work force was not allowed in the room. In October 2003, the company transferred me to the San Francisco building to oversee the Worldnet Internet room, which included large routers, racks of modems for customers' dial-in services, and other equipment. I was responsible for troubleshooting problems on the fibre optic circuits and installing new circuits.

While doing my job, I learned that fibre optic cables from the secret room were tapping into the Worldnet circuits by splitting off a portion of the light signal. I saw this in a design document available to me, entitled "Study Group 3, LGX/Splitter Wiring, San Francisco" dated Dec. 10, 2002. I also saw design documents dated Jan. 13, 2004 and Jan. 24, 2003, which instructed technicians on connecting some of the already in-service circuits to the "splitter" cabinet, which diverts some of the light signal to the secret room. The circuits listed were the Peering Links, which connect Worldnet with other networks and hence the whole country, as well as the rest of the world.

One of the documents listed the equipment installed in the secret room, and this list included a Narus STA 6400, which is a "Semantic Traffic Analyzer". The Narus STA technology is known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for pre-programmed targets. The company's advertising boasts that its technology "captures comprehensive customer usage data ... and transforms it into actionable information.... (It) provides complete visibility for all internet applications."

My job required me to connect new circuits to the "splitter" cabinet and get them up and running. While working on a particularly difficult one with a technician back

East, I learned that other such "splitter" cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.

What is the significance and why is it important to bring these facts to light?

Based on my understanding of the connections and equipment at issue, it appears the NSA is capable of conducting what amounts to vacuum-cleaner surveillance of all the data crossing the internet -- whether that be peoples' e-mail, web surfing or any other data. Given the public debate about the constitutionality of the Bush administration's spying on U.S. citizens without obtaining a FISA warrant, I think it is critical that this information be brought out into the open, and that the American people be told the truth about the extent of the administration's warrantless surveillance practices, particularly as it relates to the internet.

Despite what we are hearing, and considering the public track record of this administration, I simply do not believe their claims that the NSA's spying program is really limited to foreign communications or is otherwise consistent with the NSA's charter or with FISA. And unlike the controversy over targeted wiretaps of individuals' phone calls, this potential spying appears to be applied wholesale to all sorts of Internet communications of countless citizens. (Wired News 7/4/06)

10/ **The 10 Wackiest E-Commerce Sites.** There's much territory to explore within the four corners of the Internet, but often when it comes to online shopping, it's just too easy to rely on the mega-stores like eBay and Amazon.com. While there are hundreds of shady stores that might take your credit card number and never send you what you ordered, there are also thousands of legitimate boutiques and specialty stores plying unique wares. To help bring some diversity to your online spending sprees, Wired News asked around for suggestions in order to present you this limited, biased but gem-packed list of some of the coolest online stores.

This graphite joystick scares children, but at \$9.99, Wooters snapped them up. (Woot)Online Deals There's a bevy of choices for those obsessed with getting the lowest price, from PriceGrabber to Froogle. For those not yet jaded by rebate forms and the months spent waiting to get money back, there's free galore at FreeAfterRebate. Other great online deals can be found on the raucous boards at FatWallet and SlickDeals, which feature bargains found around the internet, sales circulars posted before publication and detailed instructions on stacking coupons and convincing store managers to price-match their competitors.

But the most fun online deals are certainly to be found at Woot.com, an online site specializing in tech products. Well, actually, product -- since Woot only sells one item a day, posted nightly at midnight Central time. Items come complete with a podcast and blog post, both of which often have little to do with the product, and a message board is packed with geeks who stay up late to cast aspersions on, say, the latest iPod speaker system. Other features include an occasional Woot-Off day, where remnants of earlier sales are offered until the warehouse is emptied. Woot's highest treasure: a Bag of Crap. The fabled and fetishized BOC costs about \$8 and includes up to three random items from the warehouse, most of it likely to be useless, but sometimes, according to legend, Woot occasionally drops in big-ticket items like a 61-inch television.

This gadget turns any table into a keyboard for your cell phone. (ThinkGeek)Gadgets At their best, gadgets are clever. Sometimes they manage to be useful, sometimes they are just downright weird, but you get way more conversational juice at a party talking about your new machine that scrambles an egg in its shell than you do fawning over how fast Photoshop loads on your shiny new dual-processor Intel Mac.

There are thousands of places to find such gizmos on the internet, but Gadget.brand.com.uk wins this round -- not simply for its wide selection of nearly useless useful things, such as a laser pointer that can also project the image of a digital clock onto a wall, but also because the site sells a USB ioniser, which purportedly releases 2 million negative ions (though no time period is specified). Think of it as a miniature version of the legendary Sharper Image air cleaner, which many users reported to be both faith-based and useful. The USB version probably works 40 times faster if your computer has USB 2.0 rather than 1.1. For those who prefer their gadgets to be a little more useful and a tad more expensive, try ThinkGeek's wide selection of geek toys and gadgets.

Designer Daniel Michalik reclaims cork for a kid's throne. (Branch) Green Eco-shopping used to mean wearing a hemp jacket and explaining to your friends how George H.W. Bush was saved in World War II by a parachute made with hemp fibres. Now, those who think green have a plethora of consumer options, from backpacks with solar panels that recharge your PSP to a site that rents hybrid electric cars online. But the prettiest green site for spending your green is Branch, a store that vends recyclable iPod nano cases, a \$3,000 table made from recycled paper, and a \$12 bonsai tree in an aluminium can.

Guilherme Marconi's neo-hippie design thrilled Threadless voters. (Threadless) T-Shirts The funny T-shirt business has moved out of the back pages of Rolling Stone and into the 21st century of commerce. There's no counting the number of T-shirt shacks lining the information superhighway, but a few stand out from the rest. Those who like shirts laced with Web 2.0 irony can clothe themselves in T-shirt stylings from Mule Design Studio. If you prefer a T-shirt that wins props at a Yeah Yeah Yeahs concert rather than an Internet cafe, try Indie Shopper. But the title of coolest T-shirt site on the net currently has to go to Threadless, which accepts design submissions, puts them up for a week of voting, then prints and sells the best ones. If that's not cool enough, you can sign up for the Threadless T-shirt club, which drops a hip shirt at your door once a month.

For the man with everything, geese make the perfect gift for a man with nothing. (Heifer.org) Philanthropic Shopping The promise of making the world a better place by buying something seems like the do-gooder's version of saving money by buying in bulk at Costco. One of the newest options is BuyforGood, a site that gets a bit of your money via affiliate programs when you shop at sites like Amazon, Target or the iTunes Music Store. All shoppers need to do is to follow the site's links to these stores, and a small portion of the purchase will be automatically sent to Buy for Good, which will send the proceeds, minus the site's overhead, to Habitat for Humanity. But long-time Internet favourite Heifer.org retains its crown. Shoppers simply choose to buy a cow, a beehive or a flock of geese, which the organization then delivers to a family in a developing country, who can tend the animals and be ensured a long-term

food supply. The only thing that would improve Heifer is if the family who gets your goat also gets a DSL line and a webcam so you could keep tabs on your philanthropy, like a 21st-century version of the letters from Africa Sally Struthers promised you in the 1980s.

This handmade scarf by part-time knitter Laura Su retails for \$30. (Etsy) Handicrafts Crafting is back, and it's turning into a big business. Those who want their woolly hats hand-knit, their thank-you cards tastefully screen-printed, and their clutches crocheted have dozens of online boutiques to choose from. Some of the better-known ones are Elsewares, Plain Mabel and buyolympia. But the blue ribbon belongs to Etsy.com, a relative newcomer whose smart web design and community-driven focus has transformed it into the handcrafter's Amazon.com. With more than 2,100 items to choose from in the knitting section alone, chances are you can find a scarf to complement any vintage dress. But if not, Etsy has a feature that lets you post a request for a custom-made item, and crafters can bid on the project.

Design and order custom parts for your hot rod, hot tub or hot house. (eMachineShop) Shopping for Making Now everyone knows that it's way cooler to roll your own cigarettes than to buy them. The recent success of magazines such as ReadyMade and Make demonstrate that it's also cooler to make your own television stand, robot or satellite dish than to fork out cash for something guaranteed to work. But even builders need supplies, and for that there are two great options. EMachineShop features online design software and instant pricing so you can get a customized widget to bolt your hybrid engine to a bicycle. Or you can just design and order your dream guitar. Spark Fun is a little less ambitious, but it's close to a one-stop shop for home tinkerers. Goodies include toy off-road tires, basic LCD displays, gyros and accelerometers. Gentlemen, start building your own robot overlord.

Retro handlebars turn standard road bikes into urban charmers. (Rivendell)Bikes The coolest online bike store wants nothing to do with carbon-fibre seat stays or Lycra tights. Rivendell Bicycle Works, a custom bike maker, believes in lugged steel frames, wool jerseys and the Brooks saddle. Its online offerings include wide, tough tires; leather straps to keep your feet on your pedals; and custom-made handlebars that will make you look like an old-time English gentleman bike racer.

These saucy shorts made from birch trees are available by subscription. (Clubfife) Underwear There's not much competition here, but what's not to love about a site that sells sexy ladies underwear made from reconstituted beechwood chips? Clubfife uses fibre called "modal," and devotees say it feels like silk but breathes like cotton. Even better, you can join ClubFife's underwear club and get your choice of two boyshorts or two low-rise thongs (NSFW) (discreetly delivered to your door for \$20 a month, shipping included).

Bamboo headphones are the new white. (Dynamism)Technology Of course, there are tons of places to buy cool electronics and other assorted computer gadgets online. It's the Internet. But it turns out that shopping for technology online is really simply the process of trying to virtually shop in Japan. Those seeking out the coolest laptops and headphones turn to Dynamism, which has the fastest and lightest laptops you can find outside the grey market. Moreover, Dynamism features bamboo and cherry wood earphones that put the nano's designers to shame.

Those who can't wait for the newest Nintendo DS game can get the Japanese release from Lik Sang, which is regularly sued for helping geographically challenged gamers. For those who just want their computer to look like it came from Japan, Pixelgirl Presents will sell you embarrassingly cute and cool sets of icons for your Mac (and sometimes Windows machine). (Wired News 20/4/06)

11/ **Who Killed the Lindbergh Baby?** When the baby son of Charles Lindbergh was snatched from his crib on a March evening in 1932, the kidnapper left a ransom note demanding \$50,000. Over the next several weeks, a dozen more ransom notes popped up, asking for bigger sums of money and telling the world-renowned aviator where to leave it. For 74 years, the notes have intrigued professional and amateur detectives alike. Who wrote them? And did the same person kill Charles Augustus Lindbergh, who was found dead two months later near his New Jersey home? A German immigrant named Bruno Hauptmann was eventually convicted of the crime and executed, partly on the basis of an FBI analysis that matched his handwriting to the ransom notes. But questions have persisted ever since.

A Virginia company thinks it may be able to solve some of the mystery for good. It is analysing the ransom notes with new software that matches handwriting samples by creating statistical snapshots of each handwritten letter and digit. If it's proven to be effective in rounds of testing, the software created by Gannon Technologies Group could do more than bring new light to an old case. It has the potential to change the American forensic landscape by providing document examiners with the same impressive degree of certainty that scientists boast of when they make DNA matches. It may be possible for the first time for someone to testify that the odds are millions to one that, say, Uncle Joe didn't sign the will that left his entire estate to his mistress.

Until now, handwriting examination "has been very much an art," said Mark Walch, director of operations at Gannon Technologies, a privately held company that specializes in optical character recognition software.

Indeed, unlike other forensic investigators, document examiners continue to rely on their eyeballs more than computers. Prosecutors and defence attorneys are aware of this fuzz factor, and they've occasionally had success challenging document examiners in court, especially since they don't come with impressive DNA-style statistics such as "there's a one in 4.5 million chance that this drop of blood came from someone other than Mr. Jones." "We just have to rely on our experience and our standard protocols," said Gary Herbertson, a retired FBI forensic document examiner who now works on his own in Berkeley, California. Instead of DNA-like odds, "We have a scale of opinions from 'certainty' and 'highly probable' to 'merely probable' and 'no conclusion.'"

Enter the handwriting analysis technology, which Gannon Technologies unveiled in February at the annual meeting of the American Association for the Advancement of Science. Armed with a bank of dozens of high-end Dell computers and a database of handwriting samples from more than 500 people who wrote a paragraph called the "London Letter" the company claims its software can easily match different samples of the same person's handwriting, even when the writer is purposely trying to fool the technology.

The key is statistical analysis that takes into account more than 200 measurements -- from curvature gradation to size -- of each letter or digit. The software then figures out which 10 or 12 of those measurements are most important, and then creates a statistical snapshot, said Donald Gantz, a statistician at George Mason University who is working on the handwriting project.

For now, Walch said Gannon Technologies is spending millions (he declined to specify the actual amount) gathering proof that the technology works. If it can be proven, the software could allow users to give odds nearly as precise as DNA analysis.

The results of the Lindbergh case ransom notes analysis, meanwhile, may be available as soon as next month, Walch said. Last year, a new handwriting analysis by the Court TV series Forensic Files suggested that Hauptmann did indeed write the ransom notes. Herbertson, the California document examiner, is intrigued by the software but is curious to see whether it picks up some common forger techniques, like tracing a signature." Personally, I like new developments," he said. "But enthusiasm for a new product should be reserved until it has suffered the test of time and practicality."
(Wired News 18/4/06)

12/ **Typo Confounds Kryptos Sleuths.** For more than a decade, amateur and professional cryptographers have been trying to decipher an encrypted sculpture that sits on the grounds of the CIA headquarters in Langley, Virginia. Three-fourths of the sculpture has already been solved.

But now Jim Sanborn, the artist who created the Kryptos sculpture, says he made a mistake. A previously solved part of the puzzle that sleuths assumed was correct for years isn't. The new information, including what the mistaken text really says, is creating a buzz among enthusiasts who've been obsessed over the sculpture for years.

It all comes down to a letter that Sanborn left out of the sculpture. He only recently realized the omission was leading sleuths down a misguided path. His followers, however, aren't feeling any grief about the misdirection. "Any time we get the sculptor saying anything for sure, it's cause for celebration," says Elonka Dunin, a game developer for Simutronics and co-moderator of a Yahoo group devoted to Kryptos who also maintains a comprehensive website about the sculpture. "We love to get any information out of him that we can."

Dunin, author of a new book of codes and puzzles that includes a couple of pages about the Kryptos mystery, said Sanborn called her Wednesday to announce the mistake. She says knowing the correct interpretation will help the group refocus its efforts and abandon dead ends its members have been pursuing since 1999. Kryptos, which means "hidden" in Greek, sits outside a cafeteria on the CIA grounds and consists of a large block of petrified wood standing upright, with a copper plate scrolling out of the wood like a sheet of paper in the shape of an S. The sculpture contains approximately 1,800 letters carved out of the copper plate in four sections, some of which form an encryption table used for deciphering the rest of the sculpture.

In 1999, California computer scientist Jim Gillogly solved three of the four sections. A CIA analyst named David Stein reached the same solution for those sections a year earlier, but his work remained unknown to anyone outside the CIA until Gillogly came forward with his solution.

The first section of the sculpture was decrypted to a poetic phrase created by Sanborn. The second refers to something possibly buried on the CIA grounds: Does Langley know about this? They should: It's buried out there somewhere. The third section is text from archaeologist Howard Carter's diary describing the opening of a door in King Tut's tomb Nov. 26, 1922. The fourth part has remained stubbornly unsolved.

The sculpture received a lot of renewed interest last year after Wired News published a story discussing author Dan Brown's references to it in the book jacket for *The Da Vinci Code*. Since then, thousands of new sleuths have been obsessing over the code. Chris Hanson, co-moderator of the Yahoo group and a Colorado programmer who runs a 3-D landscape software company called 3D Nature, created a model of the CIA's building complex, complete with landscaped grounds, to study the sculpture's surroundings for clues. Another member of the group even reportedly quit his job to devote time to cracking the code.

Sanborn has said that clues to the last section, which has only 97 letters, are contained in previously deciphered parts. Therefore getting those first three sections correct is crucial. Sanborn realized only this week that the original decryption was incorrect while doing a letter-by-letter comparison of the plain text and coded text in preparation for a non-fiction book he's producing about the life of the sculpture and the unexpected interest it's garnered.

The mistake involves an "x" that Sanborn intentionally deleted from the end of a line in section two for aesthetic reasons, to keep the sculpture visually balanced. The "x" was supposed to signify a period or section break at the end of a phrase but Sanborn removed it thinking it wouldn't affect the way the puzzle was deciphered. It turns out the "x" made all the difference. What Gillogly and others deciphered to read "ID by rows" actually should read "layer two." What that means, however, is still a mystery. "It's only eight letters and we still don't know what the rest of it says, but this is a real step forward," says Hanson. "Jim (Gillogly's) work in (1999) was the last time we got anything new out of this puzzle -- everything since then has been fruitless experimentation."

Sanborn said the error went unnoticed for years because he's avoided looking carefully at the text for fear that he would somehow leak clues about it. "I'd tried this whole process to distance myself as much as possible from the code and to not pay attention to what was going on because it helped me to not say anything," he says. "As a result this little mistake came through."

The entire passage was previously decrypted to read: This was his last message: x
Thirty-eight degrees fifty-seven minutes six point five seconds North, seventy-seven
degrees eight minutes forty-four seconds West.

ID by rows.

Sanborn said when someone first read him Gillogly's solution years ago he thought "ID by rows" was cryptographer's jargon, meant to be a notation about how cryptographers decrypted the text, not an actual part of the decrypted text. He maintained that assumption every time he saw the decrypted text re-created on websites over the years, until he did the line-by-line comparison. "Then I discovered they were, in fact, missing a clue, and it bothers me if they put 'id by rows' in instead of 'layer two,'" he says. "They didn't have everything to work with that I wanted them to have to work with."

Since getting the new clue Wednesday, Hanson has been trying to figure out the significance of "layer two." He thinks it could indicate that if one side of the sculpture is folded and layered over the other side, it will provide clues to the puzzle. "I've been drinking Mountain Dew and eating Easter Jelly Bellies to sharpen my mind," he says.

He says the new information was the equivalent of throwing a steak into shark-infested water. "There's going to be a frenzy of action around this for months because it's the first real bit of data we've been able to get. We don't know what it means. But it's very exciting." (Wired News 26/4/06)

13/ **Photo-ID card for all.** AUSTRALIANS may soon be carrying a single photo-ID smartcard for all government welfare and Medicare transactions, with senior federal ministers close to embracing the concept despite likely costs of significantly more than \$1 billion.

Senior ministers are likely to reject the introduction of a full-blown national identity card, originally proposed to bolster Australia's security. But John Howard and cabinet members including Finance Minister Nick Minchin and Health Minister Tony Abbott support a government-services smartcard, which could be announced in next month's federal budget. The card, carrying a microchip with personal details, would be required for every financial transaction with the federal Government, including family payments and the dole. It would eventually replace the magnetic-strip Medicare Card and be carried by every Australian over the age of 18.

There is a chance the card, proposed by Human Services Minister Joe Hockey, could also be extended to other government transactions, making it more difficult for welfare cheats to defraud Canberra of millions of dollars in payments.

Although stopping short of a national ID card - like the aborted Australian Card proposed in the 1980s - the new smart card has raised concerns it would impinge on an individual's privacy rights.

The Government will consider the smart card in conjunction with a national ID card, proposed following last year's London bombings. But ministers last night told The Australian a national identity card would not be implemented, despite the Prime Minister's strong initial support. "There's a lot more scepticism towards an ID card now," a senior minister said.

Ahead of the cabinet meeting today, Attorney-General Philip Ruddock will bring forward a discussion paper on the national ID card concept. But the consultant's report

is inconclusive and The Australian has learned there is only lukewarm support for the plan.

Several sources, including cabinet ministers, argue it will be too intrusive and not provide sufficient safeguards in the fight against terrorism. Even Mr Howard has gone cold on the plan. However there is considerable support for the government services card, promoted by Human Services Minister Joe Hockey.

Critics of the card argue it will be expensive to implement. Mr Hockey was asked by cabinet to commission a feasibility study on the smartcard. KPMG found in its report that it would cost up to \$2.3 billion to implement the scheme over a decade. The accounting firm admitted it was difficult to accurately project the savings -- likely to be made through clamping down on fraud -- but said they could be as much as \$1.5 billion. Mr Hockey believes it could save millions of dollars in health and welfare fraud. But critics claim such fraud has been severely reduced in recent years. Mr Hockey was last night travelling back to Australia after walking the Kokoda Track and was unavailable for comment. (news.com.au 26/4/06)

14/ **Iraqi Bloggers Comment on Nation.** BAGHDAD, Iraq -- Zeyad is a 27-year-old dentist. He works for a government clinic with broken dental chairs and no anaesthetics. At home, when gunfire rattles his neighbourhood, Zeyad's family cowers in one room murmuring prayers while he types away on his computer. Zeyad is a blogger.

Unheard of in Saddam Hussein's Iraq, blogging is providing ordinary Iraqis with a voice -- a chance to vent and reflect on the changes reshaping their country. For the outside world, the generally anonymous Internet postings offer raw insider views and insights in which sorrow and joy, hope and despair, fear and defiance coexist as the violence of the insurgency and now sectarian divisions swirl around Iraqis. "The West should listen to the opinions of the simple Iraqi people. They only hear from analysts and politicians," said Zeyad, who agreed to discuss his blogging only if his family name wasn't revealed for security reasons. "This is a good window into the world."

Zeyad typed his first entry in his Healing Iraq blog in October 2003 about Iraq's new currency, calling it "wonderful and so symbolic" that the distribution of the new dinar coincided with the anniversary of a referendum that re-elected Saddam. He has gone on to chronicle his thoughts on all aspects of life in the new Iraq.

A self-described agnostic born into a Sunni Muslim family, Zeyad reacted angrily in 2003 when the then interior minister announced that people found eating in public during the Islamic holy month of Ramadan would be detained for three days and fined. "I wanted to kill someone after reading all that," Zeyad wrote. "Free country my ass."

In later postings, he seethed at the growing influence of Muslim clerics, saying it made him fear for the future of freedom in Iraq. "I want to be able to buy my vodka without having to look left and right. I want to be able to walk with my girlfriend in the street while holding hands together without people glaring at me. Is this TOO MUCH to ask?" he wrote. "Do I have to immigrate and leave my country for wanting to do all that?"

But there were moments of pride and exhilaration, too.

One came when Iraqis voted for an interim legislature in January 2005, their first democratic election in decades. "Hold your head up high. Remember that you are Iraqi," Zeyad wrote that day. "My mother was in tears watching the scenes from all over the country," he added. "Iraqis had voted for peace and for a better future, despite the surrounding madness. I sincerely hope this small step would be the start of much bolder ones."

More recently, his blog has tackled grimmer subjects: explosions, assassinations, street fighting -- common themes in many Iraqi blogs. "Please don't ask me whether I believe Iraq is on the verge of civil war yet or not," Zeyad wrote. "All I see is that both sides are engaged in tit-for-tat lynchings and summary executions."

Zeyad said Health Ministry officials deem the trip to his clinic on the outskirts of Baghdad too risky. That's why the chairs haven't been fixed and the anaesthetics were not provided. "We don't work," he said. Still, Zeyad knows that under Saddam's regime, he couldn't have dreamed of having a blog, let alone publicly criticizing the government. Like Zeyad, who moved with his family to Britain when he was 1 and returned to Iraq at 7, most Iraqi bloggers seem relatively young and well-educated -- and they write in English.

While they often mull over the same events, their opinions vary, often along sectarian lines. Take a March 26 raid by U.S. and special Iraqi forces on a mosque compound in northern Baghdad during which at least 16 people were killed. Zeyad wrote simply that American soldiers clashed with Shiite Muslim militiamen who resisted the search, but another blogger who uses the pen name Hammurabi took a sharply different view. "American forces' crime against the worshippers," screamed a headline in Hammurabi's blog. "The killing of the worshippers in al-Moustafa mosque by the American forces should be investigated and those who are responsible for it should be punished."

Some bloggers scorn the "men in black," a gibe at Shiite militiamen accused by many Sunnis of targeting them. Others lash out at "terrorists," an apparent reference to Sunni insurgents frequently attacking Shiites. The third anniversary of the invasion of Iraq also evoked divergent emotions among bloggers. While lamenting the violence in Iraq, a blogger who uses the pseudonym The Mesopotamian praised the war that ousted Saddam. "The blood and sacrifices by the American soldiers and people will never be forgotten," The Mesopotamian wrote. "It was right, it was just and it was ordained by God that a murderer and tyrant should be overthrown."

Not really, argued a woman blogger who calls herself Riverbend. Writing in her Baghdad Burning blog, she said the war "marked the end of Iraq's independence." "I don't think anyone imagined three years ago that things could be quite this bad today," Riverbend wrote.

Riverbend's writings brought international attention to Iraqi blogging. Some of her blog entries were published in a book that is available in the United States and Britain and that won her a Lettre Ulysses Award for the Art of Reportage. Her web musings,

often critical but also sprinkled with humour, have drawn mixed reviews, with some readers questioning whether she really is an Iraqi woman. She hasn't been deterred, offering up her dismay at the hardships of daily life.

"The thing most worrisome about the situation now is that discrimination based on sect has become so commonplace," Riverbend wrote. "The typical Iraqi dream has become to find some safe haven abroad." (Wired News 23/4/06)

15/ **WorkCover loses thousands of claims.** A computer glitch has lost thousands of files on NSW workers' compensation cases.

WorkCover lost the files in the information technology collapse on March 27, Fairfax newspapers reported today. The body said no cases currently before the Workers Compensation Commission were affected. But in some cases up to 40 per cent of archival material had been lost or irretrievably corrupted, a source within WorkCover told the papers.

NSW Commerce Minister John Della Bosca said WorkCover would be asked to review its processes and make sure back-ups were kept in future.

The body investigates 13,000 cases a year. (NEWS.com.au 26/4/06)

16/ **The Evolution of Spy Tools.** Real spies may tell you that their lives are nothing like what you'd see in a Hollywood movie, but don't be fooled: They've still got some pretty cool gadgets. And aside from the relatively recent tools that monitor electronic correspondence, most of those gizmos have been around for a pretty long time. Spies claim that theirs is the second-oldest profession, and basic espionage needs haven't changed: looking and listening, getting the information they need and smuggling it back home. What has changed is the way those spy gadgets work. As technology advances and enemies get smarter, spies have had to constantly re-invent the tools of their trade.

Long before spy planes and satellites embarked upon aerial reconnaissance missions, ancient Chinese military strategist Sun Tzu (whose classic Art of War contains more than 100 references to spies and intelligence-gathering) described how secret agents could be trained to analyse enemy movements: "Dust spurting up in high straight columns indicates the approach of chariots. When it hangs low and widespread, infantry is approaching," he wrote. "When birds gather above the camp sites, they are empty."

And long before scientists knew how to reduce photographic images to the size of a printed period, American Revolutionary troops were relaying messages to one another using an invisible ink called Jay's Sympathetic Stain.

"Modern spy tools are faster, smaller, more accurate and more easily concealed," says Peter Earnest, a retired senior CIA official and the executive director of the International Spy Museum. "But they're the same basic idea as the old ones."

Over the course of human history, some amazingly complex and imaginative tools have been created. Around 500 B.C., the Spartans invented a device called the "skytale" in order to transport hidden messages. Skytales were long, slender rods that

had been wrapped with a thin strip of papyrus, leather or parchment. A message was written on the wrapping, and then the strip was unwound and passed on to a messenger (who often wore it as a belt). Only when it was rewound around a rod of the same diameter could the original message be deciphered.

In the late 15th century, Italian painter and polymath Leon Battista Alberti invented one of the first known mechanical devices for encoding messages. His so-called cipher wheel was composed of two copper disks, one slightly smaller than the other, with the letters of the alphabet etched along their edges in random order. The smaller disk was overlaid on top of the larger disk, and the two were rotated until a particular letter on one disk lined up with a different letter on the other. Messages could then be written and decoded with ease by simply substituting the appropriate letter on the other disk. A more sophisticated version of Alberti's cipher wheel was still being used 400 years later during the American Civil War.

Recently, more attention has been paid to the development of unmanned spy planes, satellites and electronic surveillance than to the efforts of human agents. But with the Cold War over and security threats less clearly defined, the individual spy is still a crucial in determining what the enemy is really thinking. And as long as they are still on the ground, they're going to need those nifty James Bond gadgets.
(Wired News 24/4/06)

17/ **People Finders / Online Privacy**

TODAY'S TOURBUS TOPICS: People Finders / Online Privacy

Today's TOURBUS is all about finding and connecting with people... whether they be long-lost friends, relatives, classmates, neighbours, co-workers or strangers. Also, learn how to find what information about YOU is publicly available online. Read on...

Research Your Family Tree

Roots, the 1977 television mini-series based on Alex Haley's book sparked a renewed interest in genealogy for many people. Back in the 70's, learning about your ancestors was a tedious job. But now, personal computers and the Internet make it MUCH easier. Here are some of the best online resources for doing genealogical research and charting your family tree...

http://askbobrankin.com/genealogy_research.html

Name and Address Search

A long-time reader recently wrote in and asked about online tools for finding people. Sherry from Birmingham said, "I'm trying to reconnect with some old friends, but I'm having trouble finding their addresses and telephone numbers. Can you tell me where

to look for good people finder tools that offer free online searches for telephone, email and address listings?"

In addition to residential and business listings for the USA and many other countries, you can do reverse lookups on phone numbers & street addresses. This means you can find a person's name and address if you know just their phone number. Or you could find someone's name and phone number if you know just the street address.

This article will tell you which people search directories I think are the best, and also what to do if you DON'T want to be found in an online directory.

http://www.askbobrankin.com/name_and_address_search.html

Is Privacy History?

What information about you is publicly available on the Web? In the past, only government agencies and businesses were able to access your personal information. Today, Internet search engines allow almost anyone to find information about friends, co-workers, job applicants, etc.

More and more info, such as property ownership, voter registration and court filings are being made available online. School, club and professional newsletters may unwittingly reveal things about you that you'd rather the whole world didn't know. What information that YOU thought was private is freely available online? Find out!

http://askbobrankin.com/is_privacy_history.html

Searching for Members in Myspace

The response to my previous articles about Myspace underscored to me that it's a hugely popular communication medium, so I'll be writing more articles to answer your Myspace questions. One reader wrote:

"I understand that once I'm logged in to Myspace I can search for people that meet certain criteria. For example, I want to locate guys over 40 within 60 miles of me that have "softball" as a searchable keyword. But HOW do I do this? I haven't been able to figure out this advanced search capability."

Finding people in Myspace is a little confusing, because there are at least FOUR ways to search for other Myspace members. This article will show you how to do basic and advanced searches, find classmates, and take advantage of the Affiliations for Networking feature.

http://askbobrankin.com/searching_in_myspace.html

(TourBus 25/4/06)

18/ **Your Thoughts Are Your Password.** What if you could one day unlock your door or access your bank account by simply "thinking" your password? Too far out? Perhaps not.

Researchers at Carleton University in Ottawa, Canada, are exploring the possibility of a biometric security device that will use a person's thoughts to authenticate her or his identity. Their idea of utilizing brain-wave signatures as "pass-thoughts" is based on the premise that brain waves are unique to each individual. Even when thinking of the same thing, the brain's measurable electrical impulses vary slightly from person to person. Some researchers believe the difference might just be enough to create a system that allows you to log in with your thoughts.

A pass-thought could be anything from a snatch of song, the memory of your last birthday or even the image of your favourite painting. A more achievable alternative might present you with predetermined pictures, music or video clips, to which you would think "yes" or "no" while the machine monitors your brain activity." It is known there are differences between people's brains and their signals," says Carleton researcher Julie Thorpe, who's working on the project with Anil Somayaji and Adrian Chan. "Can we observe a user-controllable signal encoding hundreds or thousands of bits of information in a repeatable fashion? That's the real question. We think it may be possible."

The system has the potential to become a new kind of biometric security tool that -- in contrast to fingerprint readers, iris scanners or facial recognition -- would allow users to change their pass codes periodically. But is it really feasible, or is it just another pie-in-the-sky idea?

The research is an outgrowth of efforts to build a brain-computer interface, or BCI, by trying to extract the meaningful parts of brain-wave signals measured by an electroencephalogram, or EEG, and translate them into recognizable computer commands that allow disabled people to control and manipulate prosthetic devices. A chief challenge facing BCI technology is that brain-wave signatures are unique, so a system trained to recognize a particular user can be quite difficult for another to manipulate. "Brain-wave signatures, represented as the EEG signals of a person ... are different from one individual to another, even when they perform the same thought or task," says professor Touradj Ebrahimi at the Swiss Federal Institute of Technology.

But the very distinctiveness of brain waves that works against researchers in developing universal tools is an asset when building an authentication system. A security device wouldn't need to interpret or understand the thought, but simply extract the repeatable features of the pattern and recognize a match. "A brain-based biometric can be as strong as DNA-based biometric," says Ebrahimi.

However, some researchers are sceptical that a computer will ever be able to passively recognize a particular mental image in a person's head. Iead Rezek, of the Pattern Analysis Research Group at the University of Oxford, says the proposal has "flair," but is impractical: Too many things are going on in the brain at the cellular level that all look the same from a scalp distance. "Signals from an uncountable number of nerve cells are smeared and lumped together by the time we are recording the brain-

wave patterns," says Rezek. "Authentication is akin to recognizing speakers from muffled voices because, for example, the speakers are some distance away."

Even if recognizable readings could be taken, "the link between thought and brain waves is immensely indirect," says Jacques Vidal, a BCI expert and professor with UCLA's computer science department.

Moreover, the way we remember things evolves. It may not be possible to design a system that can passively recognize the changing signature of the same thought by the same individual over time.

Vidal is more optimistic about a simpler form of mind reading, in which the computer provides a stimulus, then measures the brain's response. Such "event-related responses," or ERPs, to colour flashes or specific sounds tend to produce brain signals that are different with each individual, but nearly identical when repeated on the same person. "ERPs could be used for biometric identification," says Vidal.

Such a technique could even benefit from the adaptability of our brains. Instead of trying to passively recognize a thought, like in the ideal implementation, a system could rely somewhat on the user deliberately learning how to generate the right brain pattern, using feedback from the machine as a guide.

In experiments with monkeys, researchers found that the animal and computer can effectively train each other. "As the animal learns to control the machine, both the neurons in his brain and the algorithm that uses those signals change," says Reza Shadmehr, professor of biomedical engineering and neuroscience at John Hopkins University. "Together, the coupled system converges to a successful decoding."

For now, the Carleton group is proposing a simple, binary pass-thought system as a first step -- something similar to the brain-guided spelling devices being developed for the extremely disabled. A successful login would only occur when you are able to identify your password by thinking "yes" to the letters or pictures that form it in sequence -- like a mental game of 20 questions. If they get it working, there remain pragmatic obstacles to rolling out pass-thoughts as a replacement for other biometrics. It's easy enough to slide an index finger into a fingerprint reader, but right now the only way to tap into a person's brain signals is through a highly inconvenient EEG cap that's smeared with conductive gel and worn on the scalp.

Remote brain-activity sensors, though, are coming closer to reality every day. One company, NeuroSky, claims to have developed a non-invasive neural sensor that converts brain waves into useful electronic signals, but it's not clear when the product will be publicly available. Optical devices seem to hold more promise. "There are commercial devices now that use optics to infer neural activity near the outer layers of the cortex," said Shadmehr. "They shine a focused beam of light and measure the reflectance, and this reflection changes as the blood-oxygenation levels change. The device does not make contact with the head at all. "The technology to remotely measure brain activity is in its infancy," says Shadmehr. "Yet if we consider that it was only 40 years ago that neuroscientists developed robust single-brain-cell recording techniques in awake, behaving animals, the future for sensing brain activity is very bright indeed."

But don't throw out your passwords yet, warns the more-reserved Somayaji. "I'd be surprised and impressed if a pass-thought system was deployed in 20 years," Somayaji says. "Maybe pass-thoughts will make the transition from science fiction to science fact one day. For now, though, they're still very much science fiction."
(Wired News 27/4/06)

19/ **Chinese Man Buys eBay Fighter Jet.** BEIJING -- A Chinese businessman has bought a MiG-21f plane from a U.S. seller on the online auction website eBay for \$24,730 and plans to use it to decorate an empty space at his offices, a newspaper reported Sunday. The Beijing News newspaper identified the Chinese buyer as Zhang Cheng. "I like to collect valuable items. I have the buying power and my company has an empty space where I can display the plane," the newspaper quoted Zhang as saying.

The eBay website for the transaction shows the plane is currently located in Lewiston, Idaho. It said the fighter jet, last flown in 1995, has been inspected by a museum and found to be in excellent condition. The seller was only identified by the username "inkgrrle." The Beijing News quoted Zhang as saying he learned from the seller's son by telephone that the fighter jet was retired by the Czech military.

It wasn't immediately clear if the fighter jet can be imported into China. Zhang said he is waiting for government authorities to get back to him, The Beijing News reported. An operator at China's customs department said no one was available for comment. "There is the precedent of a Chinese company buying a retired aircraft carrier, but I don't know if this jet plane is a banned item," Zhang reportedly said. Zhang was apparently referring to the Soviet-built Minsk aircraft carrier that a Chinese company bought and converted into a floating theme park in the southern city of Shenzhen. The company went bankrupt and recently put the ship up for sale.

The report gave no indication where in China Zhang was located. EBay's government relations department didn't immediately respond to a reporter's e-mail seeking comment. (Wired News 30/4/06)

20/ **Feds' Watch List Eats Its Own.** What do you say about an airline screening system that tends to mistake government employees and U.S. servicemen for foreign terrorists? Newly released government documents show that even having a high-level security clearance won't keep you off the Transportation Security Administration's Kafkaesque terrorist watch list, where you'll suffer missed flights and bureaucratic nightmares.

According to logs from the TSA's call centre from late 2004 -- which black out the names of individuals to protect their privacy -- the watch list has snagged:

- A State Department diplomat who protested that "I fly 100,00 miles a year and am tired of getting hassled at Dulles airport -- and airports worldwide - because my name apparently closely resembles that of a terrorist suspect."
- A person with an Energy Department security clearance.
- An 82-year-old veteran who says he's never even had a traffic ticket.

- A technical director at a science and technology company who has been working with the Pentagon on chemical and biological weapons defence.
- A U.S. Navy officer who has been enlisted since 1984.
- A high-ranking government employee with a better-than-top-secret clearance who is also a U.S. Army Reserve major.
- A federal employee travelling on government business who says the watch list matching "has resulted in ridiculous delays at the airports, despite my travel order, federal ID and even my federal passport."
- A high-level civil servant at the Federal Deposit Insurance Corporation.
- An active-duty Army officer who had served four combat tours (including one in Afghanistan) and who holds a top-secret clearance.
- A retired U.S. Army officer and antiterrorism/force-protection officer with expertise on weapons of mass destruction who was snared when he was put back on active-duty status while flying on a ticket paid for by the Army.
- A former Pentagon employee and current security-cleared U.S. Postal Service contractor.
- Also held up was a Continental Airlines flight-crew member travelling as a passenger, who complained to TSA, "If I am safe enough to work on a plane then I should be fine to be a passenger sleeping."

The outcomes of these complaints are not recorded in the documents.

Attorney Marcia Hoffman with the Electronic Privacy Information Center, who obtained the documents under the Freedom of Information Act, emphasizes that "an effective redress process to clear your name from the list is critical." Currently, individuals who want to clear their names have to submit several notarised copies of their identification. Then, if they're lucky, TSA might check their information against details in the classified database, add them to a cleared list and provide them with a letter attesting to their status. More than 28,000 individuals had filed the paperwork by October 2005, the latest figures available, according to TSA spokeswoman Amy Kudwa. She says the system works. "We work rigorously to resolve delays caused by misidentifications," Kudwa says.

Citing national security, Kudwa declined to state how many of those 28,000 were ultimately placed on the cleared list, nor would she say how many names are on the no-fly and "selectee" lists or what the selection criteria for those lists are. Those on the no-fly list are banned from air travel and are likely to be arrested at the airport if they attempt to fly, while those on the selectee list face additional scrutiny at the airport.

The watch list is still not very accurate, according to 31-year-old Massachusetts resident Bethan Brome Lilja. Two weeks ago, Lilja finally grew tired of her and her son's continual selection for extra screening and contacted the TSA call centre. An employee named Eva told Lilja that the FBI was looking for someone with her name, and advised her to watch what she was saying since the call was recorded and "some guys might come knocking on your door," Lilja told Wired News. "I interpreted that as a threat," says Lilja, a full-time mother and entrepreneur. "When I call a government agency to ask for help and they tell me someone might come knock on my door, you have to take it seriously."

Lilja thinks her full name is too distinctive for it to match someone else's, and notes that her husband Jonathan does not get pulled aside for extra screening.

The TSA's lists are only a subset of the larger, unified terrorist watch list, which consists of 250,000 people associated with terrorists, and an additional database of 150,000 less-detailed records, according to a recent media briefing by Terrorist Screening Center director Donna Bucella. The unified list is used by border officials, embassies issuing visas and state and local law enforcement agents during traffic stops.

That larger list and its increasingly wide usage concerns Lilja, who wonders, for example, what will happen when she visits Canada this summer and attempts to return to the states. "If I get pulled over for speeding by some small-town cop from western Massachusetts, who sees I'm a terrorist suspect from Boston, it's hard to know if someone is going to overreact," Lilja said.

Lilja has since contacted her congressman, sought legal advice and launched an online campaign called Americans for Terror Watchlist Reform. Lilja isn't the only one interested in reforming how watch lists are used or how citizens can contest false matches or false inclusions. Currently, airlines check their own passengers' names against the lists provided to them by the TSA, but each airline chooses how it will match variations of names such as Ted, Teddy and Theodore.

For the past three years, the TSA has been trying to replace the current system, known as CAPPs, with the so-called Secure Flight program that would require airlines to forward passenger lists to the government, a process the TSA hopes will reduce the number of false name matches by standardizing the process. Some notable homeland security experts suggest, however, that more transparency and responsiveness are needed.

A paper published last year by the conservative Heritage Foundation suggested the government should establish a centralized watch-list-dispute-resolution clearinghouse that would handle complaints about all terrorism watch lists and report publicly on its work. That paper, which also advocated for the right to take watch list disputes to court, was co-authored in 2005 by technologist Jeff Jonas -- best known for his work catching casino cheats in Las Vegas and then adapting that software to enable data sharing within the federal government -- and Paul Rosenzweig, a former Heritage Foundation research fellow who recently joined the Department of Homeland Security's policy office. Rosenzweig's faith in transparency seems not to have filtered down to the TSA's Freedom of Information Office.

The Electronic Privacy Information Center filed an identical request for the 2005 complaint logs last month, but the TSA denied the organization's arguments that the records are in the public interest, and wants to charge the group nearly \$70,000 to search for the database records. EPIC is appealing that decision.

(Wired News 4/5/06)

21/ **Feds Go All Out to Kill Spy Suit.** When the government told a court Friday that it wanted a class-action lawsuit regarding the National Security Agency's eavesdropping on Americans dismissed, its lawyers wielded one of the most powerful

legal tools available to the executive branch -- the state secrets privilege. That privilege allows the government to tell a judge that a civil case may expose information detrimental to national security, and to ask that testimony or documents be hidden or a lawsuit dismissed. That extraordinary executive power was established in English common law and upheld in a 1953 Supreme Court case involving the fatal crash of a secret bomber.

In this case, the government will be asking a federal judge in California to dismiss a lawsuit filed by the Electronic Frontier Foundation against AT&T for its alleged complicity in warrantless government surveillance of its customer's internet and telephone communications. The EFF alleges that AT&T gave the government access to a massive phone billing database and helped the NSA spy on its customers' internet use.

But what exactly is the privilege, and how powerful is it?

The state secrets privilege cannot be found in the U.S. Code, the code of federal regulations or the Constitution. Instead, it is a part of common law, the body of laws and precedents created over centuries of legal decisions. When the government believes that a civil suit might reveal secrets injurious to the country, the head of the appropriate government agency must review the matter and submit a signed affidavit attesting to the danger of the lawsuit or documents that might be disclosed. Judges almost invariably agree to such requests, according to William Weaver, a law professor and senior adviser to the National Security Whistleblowers Coalition. "It's like one of magic rings from *The Lord of the Rings*," Weaver said. "You slip it on and you are invisible -- you are now secret. "Ostensibly judges could have flexibility, but they have not done that," Weaver said. "There has never been an unsuccessful invocation of the state secrets privilege when national security is involved. The (EFF) suit is over."

Weaver points to a 1978 decision by a federal court to dismiss a lawsuit against the NSA by Vietnam War protesters as a precedent for what is likely to happen in the lawsuit against AT&T.

Judges almost always accept, at face value, assertions by the executive branch about the need for secrecy, said Stephen Aftergood, who directs the Federation of American Scientists' Project on Government Secrecy. "It reflects a judicial lack of self-confidence in the face of national security claims made by the executive branch," Aftergood said. "You also see this deference in Freedom of Information Act cases."

That's a shame, according to Aftergood and Weaver, since one of the most successful ways of exposing government wrongdoing is through lawsuits. "In a nutshell, invoking the privilege shuts down the judicial process and it says that the courthouse doors are closed," said Aftergood. "In a society ruled by law, that is a subversive action."

National security could be protected, while still allowing cases to move forward, if judges allowed notes and evidence to be seen only in a special room by lawyers with security clearances -- as has happened in Guantanamo Bay criminal cases -- or if judges shut down courtrooms during sensitive sessions, according to Shayana

Kadidal, a staff attorney at the Center for Constitutional Rights, which is separately suing the NSA in an effort to stop what it calls unconstitutional wiretaps.

"The government is asserting that none of that is good enough," Kadidal said. "They are saying, 'This is so sensitive we can't rely on the judge.'"

Weaver calls that decision political. "The privilege is being used to hide criminal activity -- embarrassing activity -- and protect the president from adverse publicity and close off the investigation," Weaver said.

Charles Miller, a Justice Department spokesman, denies that the government is trying to hide any wrongdoing. "When we file certifications of the state secrets privilege, it is because it is felt that certain disclosures will be injurious to the country," Miller said. "Needless to say, the ultimate decision is by the judge."

That decision might be less predictable than the government or Weaver expects it to be. The judge handling the case, Chief Judge Vaughn Walker, is a very independent thinker, according to Hastings College of Law professor Rory Little. "He's a judge that would not have any trouble saying 'no' to any party if the law sent him there," Little said. "He's no pushover and is not predictable in a political way or in a jurisprudential way."

The assertion of the state secrets privilege is consistent with the Bush administration's culture of secrecy. The Department of Homeland Security withholds wide swaths of unclassified data that it deems Sensitive Security Information, including the internal regulation that requires airlines to ask passengers for identification.

In 2001, Attorney General John Ashcroft issued new Freedom of Information guidelines to all federal agencies that tightened the standards for deciding what information to make public. And recently, CIA chief Porter Goss fired a 20-year veteran analyst for unauthorized contact with an investigative journalist.

The FBI is trying to seize control of the notes and papers of the late columnist Jack Anderson, and in Washington, the Justice Department is using espionage statutes to prosecute two former officials of the American Israel Public Affairs Committee for discussing classified matters that they learned second-hand -- the officials never had a U.S. security clearance and were not bound by any nondisclosure agreements.

The NSA story has even spawned conjecture that the government might prosecute the New York Times reporters who broke the news, while the administration continues to fish for the identity of the whistle-blower who leaked the existence of the government's secret domestic spying program in the first place.

(Wired News 2/5/06)

22/ **Firefox Security**

Fixing a Firefox "Feature"/Security Problem

If you use Mozilla Firefox--and you should--I have something interesting to show you:

1. Launch Firefox.
2. Go to Tools > Options
3. Click on the "Privacy" padlock icon
4. In older versions of Firefox, click on the + sign next to the words "Saved Passwords." In newer versions of Firefox, just click on the "Passwords" tab.
5. Click on the "View Saved Passwords" button.
6. Click on the "Show Passwords" button.
7. When Firefox asks you if you'd really like to show your passwords, click on the "Yes" button.
8. Wail and gnash your teeth.

While it is common knowledge that Firefox can "remember login information for web pages so that you do not need to re-enter your login details every time you visit," most people don't know that Firefox stores your web passwords in PLAIN TEXT.

Should you panic? Nah. Unless you share your computer with others, the only way someone is going to be able to view your saved web passwords is if that person has access to your computer. If you have a firewall on your computer and lock your home's front door when you leave, your saved web passwords are pretty safe.

Of course, that's just my opinion. Let me add that if you share your computer with others, or if you just want to make absolutely sure your saved web passwords are significantly safer, you have three options:

1. "Throw the baby out with the bathwater": Disable the "Remember Passwords" feature in Firefox so that the program never remembers any of your web passwords.
2. "Lock down Firefox": Create a new, master password that automatically locks all of your passwords from snoops.
3. "Lock down your computer": Use your computer's user accounts feature along with a screensaver password to require everyone whose uses your computer to login.

In my humble [controversial] opinion, the last option is the best. It solves not only the Firefox saved password security problem but also a host of other security issues we don't need to go into today. How do you use the accounts feature to lock down your computer? Well, we'll get to that later.

Disable Remember Passwords

If you want to permanently disable Firefox's "Remember Passwords" Feature [which I don't recommend, but that's just me],

1. Go to Tools > Options > Privacy

2. Click on the + sign next to the words "Saved Passwords" or, in newer versions of Firefox, click on the "Passwords" tab.
3. Click on the "View Saved Passwords" button.
4. Click on the "Remove All" button. [To the Firefox gurus out there: Yes, you can do the same thing in "Clear Private Data." But you still have to go to the Passwords tab to disable "Remember Passwords." I just figured we'd take the direct route.]
5. Click on the "Close" button.
6. Uncheck "Remember Passwords."
7. Click on the "OK" button.

Doing this clears all of your old web passwords and prevents Firefox from remembering any new web passwords in the future.

Set a Master Password

Another way to lock down Firefox is to set a "Master" password. This is a special password Firefox asks you to key in once per session. Key in the correct master password and Firefox works just like it used to work by auto-filling your saved usernames and passwords on your favourite sign-in pages. Key in an incorrect master password, however, and Firefox automatically blocks your saved usernames and passwords from displaying. Sign in pages will still load, but the username and password boxes will be blank.

To set a master password,

1. Go to Tools > Options > Privacy
2. Click on the + sign next to the words "Saved Passwords" or, in newer versions of Firefox, click on the "Passwords" tab.
3. Click on the "Set Master Password" button.
4. Key in a new "master" password.
5. Click on OK.

Set Up User Accounts

How do you set up user accounts on your PC or Mac? Well, we'll talk about that next time. For now, let me throw in one extra step for you:

Update Firefox

Open Firefox and go to Tools > Options. If you see a bunch of icons down the *left* side of the screen -- General, Privacy, Content, etc.

-- YOU HAVE THE OLD VERSION OF FIREFOX which, unfortunately, is vulnerable to all sorts of nasty stuff! You really need to download the latest version at:

<http://www.mozilla.com>
(TourBus 28/4/06)

Reports since January 1999 are being placed on the NSW page of the Records Management Association of Australia Web page at <http://www.rmaa.com.au>. Any comments or ideas about these reports should be referred to the editor, Geoff Smith, at geoffsm@naa.gov.au. If people want copies of the reports e-mailed to them, please contact the editor.

If readers are interested in records management matters, then a useful developing forum for discussion is the Australian Records Management Listserv. See the RMAA webpage at <http://www.rmaa.com.au>.

If readers are interested in technology matters, then a useful forum for discussion is the Economic, Legal and Social Implications Committee (ELSIC) of the Australian Computer Society e-mail list. For further information contact Philip Argy at <mailto:pargy@acslink.net.au> or check the following Web address: <http://www.acs.org.au/index-lists.htm>

Geoff Smith ARMA AIMM GradCertMngt (Public Sector) (Macquarie)
Chair, Industry Technology and Standards NSW
Records Management Association of Australasia
8 May 2006