

Technology Issues January 2007

1/ **Media Takes on AT&T in Spy Case.** News organizations will argue Thursday that documents under seal in a high-profile lawsuit against AT&T for its alleged participation in warrantless surveillance of Americans' phone calls and e-mails should be made public. Wired News -- joined by the San Francisco Chronicle, Los Angeles Times, Associated Press, San Jose Mercury News and Bloomberg News -- is seeking documents and statements provided by former AT&T technician Mark Klein about the government spy program. AT&T says the pages contain corporate trade secrets. At 2 p.m. Thursday, both sides will make oral arguments before U.S. District Judge Vaughn Walker in San Francisco.

Wired News attorney Timothy Alger believes it's unlikely that genuine trade secrets are at issue, but argues that even if they are, the public interest in the case trumps trade-secret protections. "Even if there are trade-secrets interests, that interest has to yield to the paramount public interest in what the court is deciding," Alger said. "People should know if their phones are being tapped into by AT&T on behalf of the government." The documents at issue detail a secret switching room in AT&T's San Francisco hub equipped with internet surveillance gear. Klein provided the pages to the Electronic Frontier Foundation, which filed a class-action lawsuit against AT&T in January 2006, just a month after President Bush acknowledged the existence of the warrantless eavesdropping program.

Through a source not subject to the court's gag order, Wired News acquired and published in May documents that it believes to be near-replicas of portions of the documents under seal. Klein has publicly said the documents he's provided detail his discovery of a surveillance operation in Room 641A at 611 Folsom St. in San Francisco.

Attorney Karl Olsen, representing the other media organizations, says all the documents under seal should be published: "Even after the filing of the public, redacted version, they are still hiding the name of the city and the street with the secret room," Olsen said. "I don't think the name of San Francisco is a trade secret and I don't think any of this stuff is a trade secret."

AT&T spokesman Walt Sharp declined to comment on the media's arguments, stating simply by e-mail, "AT&T is fully committed to protecting our customers' privacy. We do not comment on matters of national security." However, in a written motion filed this summer, AT&T's lawyers derided the media's arguments: "Long on platitudes and sound-bite jurisprudence, the motion to unseal brushes aside AT&T's legitimate interest in protecting its trade secrets and the security of its network -- as if they were somehow unworthy of standing in the way of a scoop. But the case law takes the opposite attitude, recognizing that the protection of trade secrets is a 'compelling reason' not to unseal court records."

While the Bush administration declined to label the documents as state secrets, it has pushed to have the lawsuit, along with nearly 50 others targeting telecommunications companies or the government, dismissed on national security grounds. But in June, Walker ruled that the AT&T case could largely move forward since the government had already acknowledged the program, and it was clear AT&T was involved.

Walker is now overseeing all of the cases brought against telecommunications companies. In a separate case targeting the government, a Detroit judge ruled in August that the warrantless surveillance program was illegal. Federal appeals courts are scheduled to review both Walker's decision and the Detroit decision next year. (Wired News 20/12/06)

2/ **Computer Warming a Privacy Risk.** BERLIN -- A security researcher has devised a novel attack on online anonymity systems in which he literally takes a computer's temperature over the internet. The attack uses a phenomenon called "clock skew" -- the tendency for the precise clocks in modern computers to drift off of the correct time at slightly different rates, which can be affected by heat. "When a crystal is manufactured, it has a clock skew, and it's different for each crystal (throughout its) lifetime," explains Steven J. Murdoch, a Cambridge University researcher who discussed his work at the Chaos Communications Congress on Thursday.

Last year UCLA Ph.D. student Tadayoshi Kohno showed that clock skew can be used to identify computers on the internet, by charting the timestamps in a machine's traffic. But the skew is a fairly weak identifier, providing at best 64 unique fingerprints. A network of a thousand computers would have 16 with an identical clock skew. The research spawned a variety of theories on how clock skew could be used to attack anonymity online -- from detecting daytime hours at a server located in an unknown country, to counting the number of hosts behind a NAT firewall. Murdoch was the first to make an attack work.

His victim is the Onion Router, or "Tor" -- a sophisticated privacy system that lets users surf the web anonymously. Tor encrypts a user's traffic, and bounces it through multiple servers, so the final destination doesn't know where it came from. Murdoch set up a Tor network at Cambridge to test his technique, which works like this: If an attacker wants to learn the IP address of a hidden server on the Tor network, he'll suddenly request something difficult or intensive from that server. The added load will cause it to warm up.

Because temperature affects how fast most electronics operate, warming up the machine causes microscopic changes in clock skew over time. Now the attacker queries computers on the public internet that he suspects of being the Tor server, looking for the shift in skew over the course of hours. When he finds a computer that has guilty change in its timestamps, he has a match. "It's actually quite hard to defend against," says Murdoch. "(You can) lock the timestamp, but even without explicate timestamps, it's conceivable."

That doesn't mean it's time to give up on online anonymity: Murdoch points out that other attacks on Tor are currently easier and quicker. "Right now it's probably not the best attack; it's a guide to what could be done in the future." Ironically it might be the most extremely hardened computers that would be most vulnerable to this style of attack. Murdoch theorizes that military computers with precise time reporting should be easier than more casual networks like Tor, in the long run. (Wired News 29/12/06)

3/ **AT&T and Media Showdown Over Sealed Spy Docs.** A federal judge in San Francisco declined to decide today whether to unseal documents at the heart of a lawsuit against AT&T for its alleged participation in a warrantless government

wiretapping program aimed at Americans' overseas emails and phone calls. Attorneys for Wired News and print organizations argued that documents provided to the Electronic Frontier Foundation by former AT&T technician Mark Klein are of public interest. AT&T's counsel rebutted that the documents, which include detailed wiring diagrams of an alleged secret spying room in a San Francisco switching centre and an evaluation of the documents by a former FCC employee, contain valuable trade secrets and should remain under seal.

AT&T's counsel Bruce Erickson told Chief Judge Vaughn Walker that the law protected trade secrets and that the public's interest in the documents does not override that. "The documents include things important to AT&T as part and parcel of protecting its network from hackers," Berenson said.

Though Wired News independently acquired and published portions of the documents under seal in May, Berenson said the "horse was not out of the barn" and that there were sensitive technical details under seal in documents that total about 120 pages. Wired News attorney Timothy Alger contended that if the allegations that AT&T was working with the government to tap internet connections, then the public should be able to see the documents. "Given our society's reliance on the Internet, this has profound consequences if the government can intercept emails and see search engine queries," Alger said.

Karl Olsen, who represented print media outlets including the Associated Press, argued that AT&T's earlier declaration that the documents contained trade secrets was made moot by the publication of portions of the documents by Wired News. He also contended that there were no real trade secrets at issue. He cited, for example, an unredacted expert opinion that the splitters described in the documents -- which are used to siphon a copy of internet traffic into a specialized room -- are available routinely.

Vaughn Walker declined to make any decisions at the end of the two hour hearing, which was largely dominated by complex wrangling over whether a related ACLU lawsuit against AT&T and Verizon, initially filed in California state court, should stay in federal or state court. While the points of law were arcane, the government and AT&T fought hard to keep all the suits in one court, rightfully fearful that if they lost, they would be fighting on many fronts.

While neither telecoms nor the government admit they are working together as alleged in the more than 50 lawsuits filed against them, their odd legal strategy today revealed how deeply entwined their interests are. AT&T counsel Bradford Berenson, who worked in the White House on antiterrorism matters when the surveillance began, argued that letting state lawsuits go forward would imperil the government. Meanwhile Justice Department lawyer Carl Nichols argued that AT&T could get the cases moved to federal court by arguing that they were acting under the direction of the federal government.

If this case goes to state court, I can guarantee we will have soon have 50 or more cases, and [...] it will be impossible to have uniformity," AT&T attorney Berenson said. "These are the kinds of risks and dangers the United States should not have to court."

For its part, the ACLU argued that the state court has jurisdiction since the state recognizes that if AT&T or Verizon were working for the government, they are immune, but if there was no written authorization, only a request, there is no federal issue. Berenson countered that this was just a technicality and that the lawsuit is "asking a state court to enjoin an ongoing federal military intelligence program."

While Judge Walker is continuing on with smaller matters in the AT&T case, it remains largely on hold until the Ninth Circuit decides to uphold or reverse his decision to let the case go forward, despite the government's assertion that the whole case be dismissed on national security grounds. In July, Walker ruled that the case could go forward because the government has publicly admitted the existence of the warrantless wiretapping. An August decision in Detroit finding that the program was illegal is also on appeal.

The cases could also be complicated or rendered moot by planned Congressional hearings in the new year. Walker will likely issue an order on today's matter in the coming weeks. (Wired News 21/12/06)

4/ **Why You Don't Need Vista Now.** Windows Vista will have a major impact on the personal computing experience of millions of users worldwide during the coming years, but that doesn't mean Microsoft's latest operating system is a killer product, nor something you necessarily need or want.

Wired News recently obtained a copy of the final RTM, or Release to Manufacturing, build of Windows Vista Ultimate from Microsoft. This edition of the operating system is the most powerful and advanced of the four editions Microsoft will make widely available Jan. 30, 2007.

Other editions of Windows Vista are made for home users (Windows Vista Home Basic, \$200, \$100 upgrade), users who want a better entertainment experience (Windows Vista Home Premium, \$240, \$160 upgrade) and business users (Windows Vista Business \$300, \$200 upgrade). Windows Vista Ultimate (\$400, \$260 upgrade) is made for the hard-core gamer, the media collector and anyone wishing to squeeze the best performance out of drool-worthy high-end machines. Visual splendour is Vista Ultimate's greatest selling point -- the new operating system does offer a graphically intensive interface that differs greatly from that of Windows XP. Also, Vista dumbs everything down for you, streamlining the Wild West of complex OS software into a useful product. This makes tasks ranging from networking to setting parental controls a lot easier.

However, I encountered several bumps in the road during testing that show Vista is not ready for everyday use by millions of people just yet -- no matter how pretty it looks.

Installing Vista

Vista developers managed to adhere to Microsoft's tradition of making the operating system much easier to set up than the previous generation of Windows. Two decades ago, installing DOS was a delicate and risky process that often required professional help. Incremental improvements were made over the years, and Windows XP was

about as easy to install as a video game. I found that Vista coddles you even more than Windows XP did during installation.

For our tests, I used two different machines: an HP Compaq nc8430 laptop and an Advanced Micro Devices Athlon 64 PC I had built. I installed 32-bit and 64-bit versions of Vista Ultimate on two separate hard drive partitions on the Athlon desktop, and the 32-bit version on the laptop. Every installation took less than an hour to complete.

System Performance Rating Tool

Vista scans your computer when you install it and applies a performance rating to your hardware. Microsoft calls this rating the Windows Experience Index. The software then adjusts its settings to best match your hardware's score. I was humbled to learn that my AMD Athlon 64 3500+ PC with an Nvidia 6800 Ultra graphics card - - albeit with the minimum 512 MB of DRAM required just to run Vista -- merited only a 2.9 rating out of a possible 5.9. Why Microsoft chose 5.9 for the high end we may never know, but the index will be adjusted to include higher numbers (6, 7 and upward) as newer and faster hardware becomes available.

In most cases, a stand-alone graphics card is required in almost all PCs to load what Microsoft calls the "Windows Aero" visual experience, replete with Vista's enhanced translucent folders and 3-D images (However, PCs equipped with Intel's 965G Express chipset can run in Aero mode without a discrete graphics processor).

Assessed by itself, the Nvidia 6800 Ultra graphics card, which can sufficiently run high-powered games like Oblivion, rated a 5.3.1 The system performance rating is designed to give you a high-level indication of how well Vista will perform on your current hardware. This may explain in part why vendors are so excited about the new operating system. Users who want to have what Microsoft calls the "ultimate Vista experience" will have to spend a lot of money upgrading to high-end hardware components.

At the same time, whether or not you have the most beautiful graphics interface does not have much bearing on your applications. Whether your Windows Experience is rated at 3.1 or 5.1, you will probably notice little if any difference in performance while drafting a spreadsheet, using a word processor, browsing the web or even watching a DVD.

How Different Is It?

The first thing you notice about Vista when you load it up is its pretty graphics, which are still not any more beautiful than those of my equally robust (and much less expensive) SuSE Linux operating system. However, other than the new graphics, Vista's overall look and feel are not drastically different compared to XP. Vista has media, networking and other features that XP does not, but I have yet to find a single feature not already available with Linux distributions or freeware.

The e-mail software, called Windows Mail, is fundamentally the same compared to Outlook Express. Navigating the "Start" and "All Programs" menus is essentially the same.

Adding Peripherals

When I tried to plug in my peripherals, my troubles with Vista began. Since I was missing a 5.1 sound driver for my speakers, an audio device error screen appeared when I connected speakers to the PC. I had to plug in a set of headphones in place of my speakers to get the sound to work. Also, Vista didn't recognize my Hewlett-Packard Deskjet 5150 printer when it ran the initial peripheral-compatibility check. When I tried to load the printer driver software anyway, it would not install. A Google search did not reveal any readily available drivers, so I gave up. I ran into the same problem when I tried to install my Logitech webcam -- the driver wouldn't load. While the Vista version I tested is exactly what consumers will receive in January 2007, compatible drivers for peripherals might become more plentiful as the launch date approaches.

Watching a DVD

Windows Vista Ultimate comes bundled with Windows Media Centre, a package that allows you to watch and record TV (provided you have the required TV tuner hardware), burn and watch DVDs, and play video or music files. Nevertheless, many commercial software packages -- as well as freeware -- that do the same have long been available for Windows XP. I was able to immediately watch DVDs on the Athlon machine using Vista's preloaded Windows Media Centre. However, when I downloaded and installed codecs and decoders from HP's website to watch DVDs on the test laptop, my installation of InterVideo WinDVD software did not work.

Security and Privileges

Security has been one of Microsoft's key talking points when hyping Vista. Given the vulnerabilities that constantly emerge within Windows XP, who can blame the company? Wired News did not seek to exploit or discover any Vista security flaws. However, Vista does make some simple security features available that you would previously have had to install separately under Windows XP.

After setting up a user with administrator privileges, you can configure Vista to require the administrator to key in a password when new software is installed. This comes in handy when someone is logged in as another user and is not permitted to download potentially damaging software without your permission (such as the smiley faces that my 11-year-old daughter once installed to pop up in every outgoing e-mail message in Windows XP's Outlook Express). Having to key in your admin password to install software might represent an aggravation for some, but given how quickly a Windows XP machine can amass 50 or more programs -- often mixed with malware that constantly runs in the background while you are caught unaware -- I welcomed this feature.

Parental Controls

I turned on Vista's parental controls and selected them for my daughter's account. Access to certain websites -- as well as games with a mature rating -- could be blocked. When I tested this feature using my daughter's account, I found that English-language porn sites could not be accessed.

One flaw I found is that the website-blocking feature is not worth much in a multilingual home or office setting. Good ol' American porn sites were blocked, but I had carte blanche access to the raunchiest of raunchy French and Spanish sites. I was also able to use Google to search for vulgarities in those languages. I found this particularly aggravating since I live and work in France. Microsoft is able to detect my France-based IP address, and I know this because it imposes French-language web pages on me when I try to access its help sites. If Microsoft can figure out how to switch over to a French site based on my IP address, why can't it make its website-blocking feature multilingual?

Admin privileges also allow you to track the websites your kids visit and e-mails they send, among other user activities. Whether you choose to do this or not is up to you.

File Sharing

Enabling file sharing between PCs under Vista is a lot easier when compared to the often painstaking process under XP. Still, file sharing remains quirky in Vista. For example, Vista blocks you from accessing the "Set Up File Sharing" option in the "Network and Sharing Centre" menu unless you are first connected to a LAN. Only after connecting the two Vista test PCs to my LAN's router was I able to enable what Microsoft calls "Sharing and Discovery." Next, I was prompted to toggle File Sharing, Public Folder sharing and other choices on or off. After inadvertently switching all of the choices to "on" -- enabling "Password Protect Sharing" in the process -- I was blocked from accessing a shared folder from my other Vista PC when my login name was not recognized.

Sharing folders and files between a PC running Windows Vista and one running Windows XP was a royal pain. After finagling with the shared folder settings and the internet protocol, or TCP/IP, settings to enable NetBIOS over TCP/IP through Local Area Connection properties, then disabling the Windows firewall, I managed to allow a Windows XP computer to access the Vista PC's shared file folders. However, when I tried to browse shared folders on the XP machine from the Vista machine, my user name and password were rejected even after I enabled file sharing on the XP machine.

Power Consumption

Vista has garnered some initial criticism because of the ample amount of computing power it devotes to its graphics interface. At least in theory, more computing power requires more energy, which in turn eats up a notebook's battery life. Surprisingly, the nc8430 laptop's battery lasted longer with Vista running than it did with XP running. And that was without tweaking Vista's power settings to extend the battery life. During my test, I ran the laptop at full load -- complete with a sample picture menu, 10 Internet Explorer windows open and a DVD of Endless Summer playing. The battery lasted 3 hours and 5 minutes with Vista, compared to just 2 hours and 35

minutes with Windows XP. Both XP and Vista became glitchy under the load with only 512 MB of memory, but the applications managed to run.

The Verdict

Vista's power consumption superlatives aside, I would not recommend going out and buying Vista off the shelf or pre-installed on a PC when it becomes available. Users will likely suffer many headaches with missing peripheral drivers and a lack of backward compatibility with legacy software, and those headaches will not make Vista worth its hefty price tag. If possible, wait a year or more after Vista's launch to invest in the operating system. At least by then, numerous updates, hardware drivers and service packs will likely have been released.

One potential treat I hope to review in the near future is how game developers will take advantage of Microsoft's DirectX 10 API, which Vista offers. Unfortunately, DirectX 10 games and capable graphics cards were not yet available when we ran our tests. (Wired News 13/12/06)

5/ **UCLA Now Top-Ranked School for Identity Theft.** Hackers infiltrated a University of California at Los Angeles database containing personal information, including the social security numbers, of 800,000 students, faculty and administrators, according to the Los Angeles Times. The attackers, who started probing the system in October 2005, were able to get social security numbers, names and dates of birth (the trifecta for identity thieves) for an undisclosed portion of the victims before the attack was noticed and shut down in late November 2006. Today, UCLA plans to send out letters to those affected, as required by California law.

Congressman Ed Markey (D-Mass.), a champion of tighter data privacy protections, says the break-in is a reminder that Congress needs to pass a data-protection bill. Those bills have stalled on the Hill for almost two years over the standards used to decide whether a particular breach is serious enough to warrant notification and whether the federal laws will trump the growing number of state laws. Markey promised to revisit the issue next year when his party takes over Congressional committees.

The theft of personal information from a UCLA computer system is the latest reminder of the urgent need for strong federal legislation to protect consumers' Social Security Numbers and other personal information that may have been pilfered by data thieves. Almost two years after the data thefts at ChoicePoint, it is unacceptable that Congress adjourned last week without taking the necessary action to thwart data pick-pockets. While not every individual whose private information is stolen will become a victim of identity theft or fraud, all affected consumers are put in a precarious and worrisome position, wondering if at some point their information will wind up in the hands of a criminal intent on running up huge credit card bills, securing a mortgage or committing other crimes that could take years for the affected consumer to unravel. (Wired News 12/12/06)

6/ **Google Launches Patent Search.** As mentioned in the morning reboot, Google has unveiled a beta version of its new tool for searching the full text of US patent applications. Patent Search uses the same technology as Book Search, which

means you can scroll through pages and zoom in and out on text and illustrations. So far you are limited to viewing the original documents but the Google Blog says that saving and printing features will be coming soon. There's also an Advanced search feature that allows for additional criteria in your searches such as specific patent numbers, inventor name and filing dates. The advanced operators can also be used from the main search by entering the appropriate keywords like `inventor:` or `intitle:`.

Google says there are currently 7 million patents in the database and many more will be added in the future. At the moment the patents stop around the middle of 2006, but the records go back over 200 years. The records are limited to U.S. patents issued by the U.S. Patent and Trademark Office, which has its own patent search available via its website. Google claims that its conversion of Patent and Trademark Office documents makes them easier to search than the existing format. Many people may be wondering if there's really a demand to search through patents, but Google has historically done well with its niche search offerings like Books, Maps and others.

That said, patents are little more obscure but, if nothing else, enterprising journalists and bloggers can now scour the patent office for patents from Apple, Microsoft and others to see what features and products might be in the works. However, because Patent Search is currently limited to granted patents, juicy Apple or Microsoft patents that have been applied for, but not yet granted, won't be part of the results. Google's Patent Search might not be an everyday destination for most people, but the speed and familiar Google results listing page sure beats the pants off the old Patent Office search engine. (Wired News 14/12/06)

7/ **Data Spills: 100 Million Served.** Boeing's stolen laptop nudges the total number of lost or exposed personal records since February, 2005, past the 100 million mark, according to the Privacy Rights Clearinghouse's excellent data breach chronology website. The site has been diligently tracking publicly-acknowledged data spills involving information useful to identity thieves -- Social Security, bank account, credit card or drivers license numbers -- since data aggregator Choicepoint's February 2005 announcement that it exposed up to 163,000 consumers to Nigerian identity thieves.

Rapid-fire announcements this week by UCLA (800,000 records) and Aetna (130,000) moved the total to the threshold, when Boeing revealed yesterday that a laptop recently stolen from an employee's car contained names, Social Security numbers and other data on 382,000 current and former employees of the aerospace giant -- bringing the total to a grim 100,152,801 records (as of this post).

Not all those records necessarily fell into the hands of white collar crooks. Many were on misplaced backup tapes that may well have wound up in a dumpster, or on computers incidentally exposed in a hack attack, but with no evidence that the intruder had any interest or knowledge of them. Some, like the countless stolen laptops, could be in the hands of common thieves who don't know what they have, and wouldn't know what to do with it if they did.

But it all shows that corporate America -- and sometimes academia -- remains cavalier in its handling of your personally identifiable information. With the U.S. population at around 300 million, one-third of us have now been exposed through

sloppy data keeping practices -- though luckless repeat-victims presumably lower that percentage a bit. (Wired News 14/12/06)

8/ **Cyber hijackers demand ransom.** Hackers are hijacking free online email accounts, refusing to cede control unless the user pays them a ransom. Websense, a security firm that mines the internet daily for new threats, issued an alert today outlining the new form of cyber-extortion or "ransomware". Some users of Microsoft's free Hotmail email service have reported logging into their account, only to find that all of their contacts and messages had been deleted, except for one message left there by the hacker. The message, written in Spanish, roughly translates to: "If you want to know where your contacts and your emails are then pay us or if you prefer to lose everything then don't write soon!"

The hacker doesn't specify a ransom amount, presumably so that they can negotiate a maximum amount with each individual target. Joel Camissar, Websense's Australia and New Zealand country manager, said while he was not aware of reported cases where the attacks targeted Australians, he expected it to spread quickly to English-speaking countries. "At this stage it is not a significant number of people that seem to have been infected," said Mr Camissar.

It is understood that the hackers gain access to the email accounts by infecting internet cafe computers with a keystroke logger, allowing them to obtain the username and password of each person that logs in. "From my cursory understanding of this type of threat, it was reported back to us that the end-users had transacted at an internet cafe, where their credentials may have been compromised," said Mr Camissar.

According to Mr Camissar, this signals a second wave of cyber-extortion. He said the first wave appeared back in May last year. "The first ransomware we detected was a Trojan horse that encrypted documents on a user's PC, and you needed to receive the decryption code from the hacker by depositing up to \$250 in their bank account," he said. "This [the Hotmail attack] is a more sophisticated type of ransomware, because rather than relying on a user to be infected by a virus themselves, all the user needs to do is type in their credentials on a computer that is not secure." Mr Camissar said that he was not sure whether the hackers would restore the user's account when paid, but said his previous experiences with ransomware attacks suggested they would keep to their word. (smh.com.au 13/12/06)

9/ **SMS to double by 2010.** TEXT messages sent to and from mobile phones will more than double over the next five years to 2.3 trillion messages sent by 2010, a survey said. The number of messages transmitted over short message service (SMS) systems in 2005 was estimated at 936 billion, according to British market research group Gartner. Total revenues from text messaging is forecast to grow to \$US72.5 billion (\$8.92 billion) in 2010 from \$US39.5 billion in 2005.

"By far the most messages will continue to be sent in the Asia Pacific region, where Gartner predicts the level of SMS messages will top 1.8 trillion in 2010," it said in a statement. "Wireless messaging is the most successful mainstream mobile data service to have emerged during the 30-year history of the cellular telecoms industry," it added.

Gartner said new messaging services are needed, including instant messaging, picture messaging and video messaging, but they would only match the popularity of SMS if they are simple to use and affordable, which are the reasons behind SMS success. (Australian IT 13/12/06)

10/ **European Citizens Have More Privacy Rights in U.S. Tracking System than U.S. Citizens.** There's been a long-standing and typically European bureaucratic battle between the United States and the European Union over having airline passenger records sent from flights originating in E.U. countries that are headed to the United States. It's mostly crap that revolves around the Europeans having a stricter data protection law that they never enforce, but like to pretend is better than U.S. rules. But they did strike a deal that gives E.U. citizens some measures of protection and limitations that U.S. citizens do not enjoy when it comes to the Automated Targeting System. (I won't bore you with the details of the negotiations, but the most recent agreement simply continues the original 2004 agreement.

In short, U.S. Customs and Border Patrol get fewer fields of data on E.U. citizens, can't get at data that could show ethnicity, racial origin, health problems, political affiliation or union membership, can't share the data very widely with other law enforcement and intelligence agencies, and must destroy the data in years rather than four decades.

DHS spokesman Jarrod Agen declined to comment on why that E.U. citizens have significantly higher data protection rights than U.S. persons, since he disagreed with the characterization. He says the U.S. is "comfortable" with the data fields it is getting, but that it does want the next round of negotiations to remove the strict limits.

Agen said that the differences in data storage aren't real yet, since the agreement is still so new that none of the E.U. data has yet been moved to the destroy pile and that the U.S. is pushing to have longer storage times since terrorist plans take 5 to 10 years to develop.

Agen also said that the notion that the government stores a "score" on travellers is incorrect. Instead the system works by noting a suspicious item -- say that a traveller has an address in his airline record that matches an address in an intelligence database record for a suspected terrorist. Then at the border, an agent can question that person, who might then say that they lived at the address years after that messy terrorist moved out. That information would be noted in the system, Agen said, so that the person doesn't get repeatedly stopped. He did not know however if the database kept information on when and why a person got stopped previously. He could only confirm that it would keep the airline data. (Wired News 13/12/06)

11/ **800,000 hit by UCLA hack.** A hacker has infiltrated a massive University of California, Los Angeles database containing personal information on 800,000 people in one of the worst computer breaches ever at a US university. The highly sophisticated attack exploited a software flaw to crack the computer system in a bid to obtain Social Security numbers, UCLA said in notices sent to all 800,000 potential victims, most of them current or former students and faculty members.

The University had no suspects despite an emergency investigation that began shortly after the hack was discovered on November 21, said Jim Davis, UCLA associate vice chancellor of information technology. The FBI has also begun a probe. "We definitely do not know who it is yet," Mr Davis said. "All indications so far are that this is a malicious, targeted attack and well orchestrated. And the other thing that was unnerving to us was that it was orchestrated in such a way so that it covered its tracks." Mr Davis said the hacker apparently began trying to worm into the system more than a year ago but drew suspicion only after technicians investigating performance issues on the computer system noticed odd "data traffic patterns".

The database contained names, social security numbers, dates of birth, home addresses and contact information that could be used by identity thieves. Access is normally restricted to UCLA staff whose jobs require them to have access. The university said it was not aware of any instance in which the personal information had been "misused" but was notifying all 800,000 people as a precaution. Mr Davis said the school was also reviewing its practices for storing personal information.

In addition to 38,000 current UCLA students and 25,000 faculty members, the database apparently stored personal information for many former students going back at least a decade. University spokesman Phil Hampton said the database was not used for fund-raising and that in some cases federal law required the school to maintain the information.

Computer security experts told the Los Angeles Times the sheer number of people exposed to the hacker made it one of the largest ever perpetrated against an American university. In 2005, a database containing 270,000 names was infiltrated at UCLA's cross-town rival USC. Earlier this year, a US Veterans Affairs laptop containing data on 26 million veterans and service members was stolen from a staffer's home. (Australian IT 13/12/06)

12/ **DHS Passenger Scoring Illegal?** WASHINGTON -- A newly revealed system that has been assigning terrorism scores to Americans travelling into or out of the country for the past five years is not merely invasive, privacy advocates charge; it's an illegal violation of limits Congress has placed on the Department of Homeland Security for the last three years.

The Identity Project, founded by online rights pioneer John Gilmore, filed official objections to the Automated Targeting System, or ATS, on Monday, calling the program clearly illegal. The comment cited a little-known provision in the 2007 Homeland Security funding bill prohibiting government agencies from developing algorithms that assign risk scores to travellers not on government watchlists. "By cloaking this prohibited action in a border issue ... the Department of Homeland Security directly and openly contravenes Congress' clear intent," wrote project members Edward Hasbrouck and James Harrison.

A DHS spokesman said the language in the appropriations bill doesn't cover the ATS, and insisted the program is legal. At the National Targeting Centre, the ATS program harvests up to 50 fields of passenger data from international flights, including names, e-mail addresses and phone numbers, and uses watchlists, criminal databases and other government systems to assign risk scores to every passenger. Though the

government has provided few details, such a system could look at travel history, who the ticket was purchased from or what kind of car someone drives to attempt to figure out who is a likely terrorist threat. When passengers deplane, Customs and Border Protection personnel then target the high scorers for extra screening. The notice says the data and the scores can be kept for 40 years, shared widely, and be used in hiring decisions. Travellers may neither see nor contest their scores.

Paul Rosenzweig, a high-level Homeland Security official, told Congress in September that the system had "encountered 4801 positive matches for known or suspected terrorists." However, it is unclear how many of those were correct matches.

The system appears to fly in the face of legal requirements Congress has placed in the Homeland Security appropriations bills for the last three years, which states, "None of the funds provided in this or previous appropriations Acts may be utilized to develop or test algorithms assigning risk to passengers whose names are not on government watch lists." The prohibition most recently appeared in section 514(e) of Congress' 2007 appropriation, which was signed into law by President Bush on Oct. 4th. It's one of a set of restrictions on the long-delayed and scandal-plagued replacement for the current domestic air travel watchlist system.

Planned replacements would have the government, not airlines, check passengers' names against watchlists. An early version called CAPPs II would have assigned colour-coded threat levels to passengers determined by a mix of government and commercial data, but that was scuttled by the DHS after the plan was widely criticized.

Marc Rotenberg, the director of the Electronic Privacy Information Centre, said he was unaware of the language but that it clearly applies to the Automated Targeting System, not just Secure Flight, the delayed successor to CAPPs II. "Bingo, that's it -- the program is unlawful," Rotenberg said. "I think 514(e) stands apart logically (from the other provisions) and 514 says the restrictions apply to any 'other follow-on or successor passenger pre-screening program'. It would be very hard to argue that ATS as applied to travellers is not of the kind contemplated (by the lawmakers)."

Jim Harper, a Cato Institute fellow who also serves on the DHS' external privacy advisory board, echoes Rotenberg's reading. "The language is clear that the risk scoring may not be used on non-suspects," Harper said. "The counter-argument is that the section it is in is about Secure Flight, but I think you have to pretzel yourself to make that argument."

The government could still check passenger names against watchlists and criminal databases for possible matches, according to Harper's analysis. "But it certainly makes the use of risk-scoring unlawful, I suspect," Harper said. DHS spokesman Jarrod Agen disputes that interpretation. "The language in the appropriation bill refers specifically to Secure Flight," Agen said. "The authority for ATS is all mandated by the Aviation and Transportation Security Act, which mandates that we receive the airline data and interpret that data to keep terrorists out of the country."

Details of the program were first announced in early November in the Federal Register, but gained more attention when the Associated Press reported that the

system began operation prior to 9/11. Privacy activists say they knew nothing about the program since they assumed it was simply being used to screen cargo. The Identity Project requested that all current records in the system be destroyed and that the program be re-configured. The comment period on the proposal, which ended Monday, will be re-opened on Friday for additional feedback. Comments can be submitted online using docket number DHS-2006-0060. (Wired News 7/12/06)

13/ **Bush 'Privacy Board' Just a Gag.** WASHINGTON -- The first public meeting of a Bush administration "civil liberties protection panel" had a surreal quality to it, as the five-member board refused to answer any questions from the press, and stonewalled privacy advocates and academics on key questions about domestic spying.

The Privacy and Civil Liberties Oversight Board, which met Tuesday, was created by Congress in 2004 on the recommendation of the 9/11 Commission, but is part of the White House, which handpicked all the members. Though mandated by law in late 2004, the board was not sworn in until March 2006, due to inaction on the part of the White House and Congress. The three-hour meeting, held at Georgetown University, quickly established that the panel would be something less than a fierce watchdog of civil liberties. Instead, members all but said they view their job as helping Americans learn to relax and love warrantless surveillance. "The question is, how much can the board share with the public about the protections incorporated in both the development and implementation of those policies?" said Alan Raul, a Washington D.C. lawyer who serves as vice chairman. "On the public side, I believe the board can help advance national security and the rights of American by helping explain how the government safeguards U.S. personal information."

Board members were briefed on the government's NSA-run warrantless wiretapping program last week, and said they were impressed by how the program handled information collected from American citizens' private phone calls and e-mail. But the ACLU's Caroline Fredrickson was quick to ridicule the board's response to the administration's anti-terrorism policies, charging that the panel's private meetings to date largely consisted of phone calls with government insiders and agencies. "When our government is torturing innocent people and spying on Americans without a warrant, the PCLOB should act -- indeed, should have acted long ago,"

Fredrickson said. "Clearly you've been fiddling while Rome burns. This board needs to bring a little sunshine. So far America is kept in the dark -- and this is the first public meeting you have had."

Lisa Graves, the deputy director of the Centre for National Security Studies, asked the board two simple questions: Did they know how many Americans had been eavesdropped on by the warrantless wiretapping program, and, if so, how many? Raul acknowledged in a roundabout way that the data existed, but said it was too sensitive to release. Graves then asked if the board had pushed to have that data made public, as the Justice Department is required to do with typical spy wiretaps. Raul declined to say. "It is important for us to retain confidentiality on what recommendations we have and haven't made," he said.

Graves tried to push the issue of whether the board was going to be public or private, but chairwoman Carol Dinkins politely cut her off and ended the question-and-answer session.

Board member Lanny Davis, who had introduced himself by saying he grew up in a household where the ACLU was considered a "heroic organization," jumped in to explain why the nation's most prominent privacy board won't be transparent about whether it is urging more transparency. "Congress put us in the office of the president, we didn't," Davis said. "Had Congress wanted us to be an incensement agency, it would have made us independent."

The sparsely attended meeting shaped up as a mostly one-way conversation, with attendees offering suggestions on how the board could transform itself into an effective organization by building on the work of earlier government privacy panels.

Fred Cate, a cybersecurity professor at Indiana University, stressed that anti-terrorism programs that collect and sift through data on Americans -- such as the no-fly list and the recently announced Automated Targeting Centre that has been computing terrorism quotients for those flying in and out of the country for more than five years - - need to have a robust way for people to contest the scores and underlying data. "Redress seems to be the foundation of any system," Cate said. "The only certainty in this entire field is that there will be false positives."

The committee members largely kept their views to themselves, and the press was barred from posing questions during the two short public question periods. Dinkins, the board's chairwoman, who is a partner at the same law firm where Attorney General Alberto Gonzales once worked, offered little beyond pleasantries. Another board member, Francis Taylor, never spoke. (Wired News 6/12/06)

14/ **MySpace to Purge Sex Offenders.** MySpace announced today it will begin searching its 100 million-plus user list for people listed in a national database of sex offenders. Why didn't I think of that! Just kidding. Obviously, this is a response to my story from October. If you missed it, I used a Perl script to screen-scrape the Department of Justice's National Sex Offender Registry and run all the names and ZIP codes through MySpace's search engine, verifying 744 matches from half the search results. One convicted child molester was actively courting new victims, and was arrested.

Now MySpace is going to do its own searching, in partnership with a background-check company called Sentinel Tech Holding Corp. From the press release:

"We are committed to keeping sex offenders off MySpace," said MySpace's Chief Security Officer, Hemanshu Nigam. "Sentinel Safe will allow us to aggregate all publicly available sex offender databases into a real-time searchable form, making it easy to cross-reference and remove known registered sex offenders from the MySpace community. The creation of this first-of-its-kind real-time searchable database technology is a significant step to keep our members as safe as possible."

The whole first-of-its-kind, never-been-done-before, thank-God-the-technology-finally-exists thread runs throughout the press release. The language seems calculated

to let MySpace escape responsibility for failing to police the sex offenders on its site prior to October, despite the availability of a free online registry demonstrably useful for exactly that purpose.

That said, Sentinel's database promises to be far more powerful than the DOJ registry I used. As described, it'll contain detailed information, including height, weight, eye and hair colour, and the complete offence history of each offender -- all completely searchable. It'll be like a Google for sex offenders. That leaves just one real disappointment in this announcement: How MySpace plans to use the data. With all that information at its disposal, and a "24-hour-a-day dedicated staff" using it, MySpace could seriously enhance its policing.

Instead, the company is taking a sophisticated database and wielding it as a blunt instrument, simply banning everyone on the list from registering or keeping a MySpace account, regardless of who they are or what they did. This is bad because, obviously, banning sex offenders won't keep them off MySpace: it'll just give them a reason to lie about their name or location, even if they aren't up to no good. (My survey found hundreds of past offenders, many with old or minor convictions, whose profiles reflected a seemingly normal life.) Now sex offenders who want to stay on MySpace will all be using false information from the start.

MySpace is essentially refusing an opportunity to detect and imprison active repeat offenders, by moving the entire superset of ex-offenders into the shadows. Does the convicted paedophile have lots of teenagers on his friendslist? MySpace won't know, because he'll be under same veil of anonymity as the flashers and peeping toms.

We know there are some ex-sex offenders who attempt to recidivate from accounts opened under their real names. If you believe they will now stay off MySpace, then the company's policy is good for safety. But if you think they'll simply start spelling their name a little different or lying about their ZIP code, then MySpace has lost the chance to take them off the streets. MySpace is taking the easy way out. It may be good PR to be able to say that you don't allow past sex offenders of any stripe on your website, but the company should keep its eye on the ball: the goal isn't to keep a former flasher from blogging about his cat, it's to keep current paedophiles from pursuing children.

MySpace could tell the difference, if it wanted to. A smart policing effort would use the sex offender database as one of many data points in keeping the site safe. Sometimes zero-tolerance is really tolerance. (Wired News 5/12/06)

15/ **Zune Comes With Porn Value-Add.** Umm, this isn't exactly what we were suggesting, Microsoft, when we advised improving the Zune user experience. A Chicago-area mother reports that the supposedly new Zune she bought her 12-year-old daughter for Christmas was stuffed with pornography, specifically "a homosexual orgy they had videotaped for an hour and 44 minutes." The mom is pretty certain the player, which she purchased from a nearby Wal-Mart, was an unmarked returned unit. Besides the porn, she notes there was no charging cord in the box. The store manager, however, "blamed it on Microsoft." The mom got her money back, a \$25 Wal-Mart gift card and very uncomfortable discussion with her daughter.

We feel obliged to note how much worse it could have been if Microsoft had been at fault. At the risk of making our valued readers toss their lunch, think of Steve Ballmer. And porn. "Developers, unhhhh, developers...." (Wired News 21/12/06)

16/ Clues To How the NSA Spies on Americans and Possible Immunity for Telecoms for Helping Gov Spy. Those who like to read tea leaves to figure out how the Administration actually captures Americans' emails and phone calls without a warrant may have gotten a more cups to look at this week, even as telecom lobbyists are reportedly working hard to have Congress let them off the hook from pending lawsuits for their participation.

On Tuesday when the White House's Privacy and Civil Liberties Oversight Board met for the first time, the five members, who all had been briefed on the NSA program in November, didn't reveal much. In fact, Board member and former Solicitor General Theodore Olson remain mum until the final panellist suggested a way to avert a looming Constitutional showdown over whether the president has the inherent power to wiretap Americans without a warrant in the face of an external threat to the country. (The Supreme Court has already ruled the President has no such authority with regards to domestic threats.) That piqued Olsen's attention. More including some speculation on the meaning of another bill introduced by Specter to legalize the program after the jump...

Olsen, whose wife was on the plane that terrorists crashed into the Pentagon on 9/11, expressed interest in the suggestion that the nation's surveillance laws could be modified to add a specialized, and more limited, warrant to wiretap an American when all the government has is a suspicion they are involved with terrorism or spying. The idea was floated by Anthony Clark Arend, a Georgetown law professor.

Currently, the law requires probable cause to get wiretap approval. Olsen's interest may show that the real reason the Administration launched the secret program outside of the law was the level of suspicion necessary to get a warrant, not the slowness of the warrant process, as the Administration has publicly stated.

Senator Dianne Feinstein (D-Ca.), who as a member of the intelligence community was briefed on the program, has long contended that the program could and should use the regular warrant process. So the problem may be, as panellist Peter Swire (Clinton's privacy czar) surmised after the meeting, that the program isn't such a dragnet that it couldn't use warrants, it's just that there's no way to get a warrant when you only know a phone number or have the name of someone who called someone who called a suspected Al Qaeda member (those examples mine, not Swire's).

So if Congress can find a way to create a more limited warrant -- such as one whose info can't be used in prosecution or lasts not as long -- and requires that a more full warrant be gotten later that might satisfy the administration and more moderate critics, who are less concerned with the surveillance than the fact it happens unilaterally. Then as commenter EJ pointed out on Tuesday Senator Arlen Specter introduced yet another bill that would change the nation's wiretap rules to accommodate the program, though in response to ongoing court challenges the new bill drops changes that would have moved such challenges to a secret court.

The most interesting parts are here:

SEC. 203. INDIVIDUALIZED FISA APPLICATIONS.

The contents of any wire or radio communication sent by a person who is reasonably believed to be inside the United States to a person outside the United States may not be retained or used unless a court order authorized under the Foreign Intelligence Surveillance Act is obtained.

SEC. 204. ISSUES RESERVED FOR THE COURTS.

Nothing in this Act shall be deemed to amend those provisions of FISA concerning any wire or radio communication sent from outside the United States to a person inside the United States. The constitutionality of such interceptions shall be determined by the courts, including the President's claim that his article II authority supersedes FISA.

Now Specter has long complained that he doesn't know anything more about the program than the rest of the country does, since he's never been briefed on the classified program (not being on Intelligence committee).

So this language may come from the White House, since there is no other reason for him to believe that the gov should and could get a warrant for outgoing international communications, but not for incoming calls. So one might surmise the program is really focussed on all incoming calls from certain locations, say Pakistan or Afghanistan, then the NSA spooks and algorithms sort through them to find the interesting ones and then the government can have enough info to get a proper warrant.

Of course that's all tea leaf reading, but it might just be right.

As for immunity provisions for the telecoms, I hear tell it's still not dead and that the tax break bill that Congress is highly likely to pass may be the vehicle. It's not clear if what's being considered will be a total immunity provision or a change to substitute the government for the telecoms in all the 48 or so pending lawsuits against the telecoms. That change would give the government the ability to assert not only the state secrets privilege but also executive privilege and sovereign immunity, which would be almost impossible for any plaintiff to overcome in court.

(Wired News 7/12/06)

17/ **Cheaper Gas Hurt Hybrids.** As gas prices retreated this fall so did the sales of hybrids, but both phenomenon are likely to quickly reverse course. According to the San Francisco Chronicle, all passenger car sales dropped 19 percent in November, while hybrid sales dropped even faster at 31 percent. Gas prices fell in late October, but as fast as you can say "midterm election" the price of oil coincidentally started rising after the first Tuesday in November. In Phoenix, gas prices rose 11 cents per gallon in early November. I am not saying, really, that there is cause and effect here, it's just happenstance that the folks who want to see Republicans in power would lower their prices before an election.

While the Chronicle says that the halving of the tax credit available to Toyota Prius buyers (a tax quirk that penalizes the companies that sell the most hybrids) could be hurting sales, Toyota sold more Prius' than ever in November, over 8,000 units.

Gasoline prices are not likely to hover around \$2.30 for long, and hybrid sales will probably remain stable or grow as more options hit the market. The new Congress may extend the hybrid tax breaks to prompt continued sales. (Wired News 5/12/06)

18/ **Fingerprinting da Vinci.** Anthropologists believe they have captured Leonardo da Vinci's fingerprint after combing through the artist's work, the Associated Press reports. The reconstructed print, supposedly from Leonardo's left index finger, could help researchers confirm the master's touch on disputed works and might even shed light on his parents. "It adds the first touch of humanity," said anthropologist Luigi Capasso of Italy's Chieti University. One bonus for researchers: Leonardo apparently ate often while working, so his fingerprints might contain saliva or other biological materials. (Wired News 2/12/06)

=====

Reports since January 1999 are being placed on the NSW page of the Records Management Association of Australasia Web page at <http://www.rmaa.com.au>. Any comments or ideas about these reports should be referred to the editor, Geoff Smith, at geoffsmith@unwired.com.au or geoff_smith98@hotmail.com. If people want copies of these reports emailed to them please contact the editor.

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

Readers interested in technology matters then a useful forum for discussion is the Economic, legal and Social Implications Committee (ELSIC) of the Australian Computer Society email list. Check the following Web address at <http://www.acs.org.au/index-lists.htm>.

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

6 January 2007