ICANN's Whois Privacy Reforms Stalled Again
Computerworld (08/28/07), J. Vijayan

ICANN's workgroup dedicated to solving differences over proposed privacy changes to the Whois database has failed to develop a proposal for reforming the way Whois data is handled. The failure to reach an agreement perpetuates a long-standing holding pattern on proposed reforms to how Whois data is managed. GoDaddy's T. Ruiz says the Whois debate has been ongoing for years and it is time for ICANN to bring it to a conclusion. "It's been clear for some time that unanimity, or even consensus, on any changes is not possible," says Ruiz. Ruiz was part of the 60-person working group, which included service provider representatives, registrars, and law enforcement authorities. Companies, intellectual property holders, and law enforcement officials support open access to the Whois database as it helps find phishers, trademark and copyright violators, and other online criminals. Privacy advocates believe unrestricted access could expose individual domain registrants to spam and unwanted surveillance and argue that Whois should be shielded from public access. The Whois task force has been working for more than four years to address the concerns of all sides involved and recently came up with the Operational Point of Contact (OPoC) proposal, which would allow domain name registrars to continue to collect contact information but would require them to prevent public access to the database, except in cases where law enforcement authorities and other parties could demonstrate a valid need for access. The OPoC proposal failed to gain support, partially because of how access proposals would be handled and concerns over who should be able to access protected Whois data and under what conditions.

UTEP Awarded $5 Million to Create Cyberinfrastructure Center
University of Texas at El Paso (08/21/2007)

The National Science Foundation has awarded a $5 million grant to the University of Texas at El Paso to establish a cyberinfrastructure center. Experts in computer science, mathematics, and earth and environmental sciences will use the Cyber-ShARE Center of Excellence to develop software applications, services, and other digital tools that will help improve the nation's cyberinfrastructure. Scientists will be able to use the applications developed by researchers at Cyber-ShARE to gather and compute data over the Internet for projects. "Traditionally, research is done at large institutions throughout the world and it's difficult to share information others are working on," says A. Gates, chair of UTEP's Dept. of Computer Science. "But the whole promise of cyberinfrastructure is that it breaks down those boundaries and allows scientists and educators to do state-of-the-art research." Cyber-ShARE will also make its information and applications available to the public, provide opportunities in Web-based research to college students, and offer outreach programs to middle and high school students and teachers.

House to Consider E-Voting Reform Bill
Computerworld (09/05/07), G. Gross

The Voter Confidence and Increased Accessibility Act, introduced by Rep. R. Holt (D-N.J.) could be taken up by the House this week. Holt's bill would require a voter-verified paper ballot for the November 2008 election as a way to audit voting results. There would be random audits of e-voting machines in 3% of precincts, and e-voting machines would not be able to have wireless or Internet connections. Although the bill has 216 cosponsors, its passage is not assured because some groups oppose the move away from existing e-voting machines. Even if it passes the House, there is no guarantee a similar bill in the Senate will pass, says the Electronic Frontier Foundation's M. Zimmerman. "Like it or not, with election officials arguing that they're running out of time to implement wholesale changes, this likely amounts to Congress' only attempt to make any serious improvements to the nation's election procedures ahead of the 2008 presidential election," Zimmerman writes in his blog.

DHS Head: Cybersecurity Remains a Concern
IDG News Service (09/05/07), G. Gross

M. Chertoff, Secretary of the US Dept. of Homeland Security, spoke before the House of Representatives Homeland Security Committee and testified that DHS will continue to give the "very big issue" of cybersecurity high priority. Because the department's cybersecurity endeavors are confidential, Chertoff simply made a short statement to assure committee members that DHS is collaborating with other parts of the government to develop an improved strategy for cybersecurity. Chertoff also acknowledged that threats to cybersecurity have great potential to harm the United States in the future. Though cybersecurity problems continue to plague the federal government, the legislators primarily focused on other issues during the meeting, urging DHS to improve in other ways, such as by filling open positions at DHS.

Cyber Crime Tool Kits Go on Sale
BBC News (09/04/07)

Novice cyber criminals can now develop their own cyber attacks with the help of automated, easy-to-use tools and kits developed by malicious hackers. There are at least 68,000 downloadable hacking aids currently circulating, says Secure Computing's P. Henry. Although most are free and targeted toward those with expertise, a growing number are for sale and aimed at unskilled individuals. Some hacking groups offer virus-writing services that generate individual malicious programs, while others have created expensive kits that even come with technical support to keep the software updated with the latest vulnerabilities. One such product, Mpack, was used in June to subvert over 10,000 Web sites in one attack. The tools are effective because it takes a substantial amount of time for security professionals to patch the increasing number of vulnerabilities being discovered. Hacking groups are drawn to selling such products because doing so confers little risk upon them, as each tool comes with a disclaimer stating that the user assumes responsibility for any abuse.

House Puts Off Voting Bill, Most Other Business Next Week
CQPolitics.com (09/07/07), K. Hunter; A. Ota

Debate on a House bill that would require all electronic voting machines to provide a paper record of every vote cast was postponed until September 17th at the earliest due to a short work week for Congress. House leadership had planned to bring H.R. 811 to the floor for debate on Monday, but a planned Rules Committee meeting for Friday that was to discuss amendments to the bill and a debate schedule was canceled. Local election officials opposed to the bill say the delay is a temporary victory that could lead to the bill's demise. However,

supporters of the bill say the delay was made to accommodate the House calendar. "There's been concern about this bill for four years," says an aide to Rep. R. Holt (D-N.J.), the bill's chief sponsor. "But I think it's clear at this point that the momentum is moving in the right direction." Still, aids say that a recent Congressional Budget Office review of the bill, which found that it would cost $8.4 billion over 10 years to implement, will force lawmakers to rework the bill to cover its costs. Meanwhile, House Rules Chairwoman Rep. L. Slaughter (D-N.Y.) said an amendment for the bill was needed to provide an exception for New York, which the federal government sued for failing to meet a 2006 deadline to replace lever voting machines. If the amendment passes, New York would have until 2010 to add a paper ballot backup system. And Rep. D. Moore (D-Kan.) may try to add an amendment that would postpone deadlines if funds are not appropriated to states to help pay for new requirements.

F.B.I. Data Mining Reached Beyond Initial Targets
New York Times (09/09/07) P. 1; E. Lichtblau

Newly obtained FBI documents show that the bureau's data mining efforts to find data on terrorism activities was more widespread than originally thought. The FBI relied on telecommunications companies to analyze phone-call patterns of the associates of Americans who had come under suspicion, creating a "community of interest" that could implicate innocent Americans in investigations. The bureau stopped using this practice early this year, partially because of broader questions on its aggressive use of the records demands, known as national security letters. The community of interest data is important to a data-mining technique known as link analysis, which uses communications patterns and other data to identify suspects who may not have any other known links to extremists. Supporters of the system say it is a vital tool in predicting and preventing attacks, but privacy advocates, civil rights leaders, and even some counterterrorism officials say link analysis can be misused to establish links to people who have no real connection with terrorism. The FBI declined to say exactly what data was examined, but a government official, speaking on the condition of anonymity, says the data was limited to people and phone numbers "once removed" from the central target. The FBI's M. Kortan says that community of interest data is "no longer being used pending the development of an appropriate oversight and approval policy," and that the technique was used infrequently and was never used for email communications.

Storm Worm Botnet More Powerful Than Top Supercomputers
InformationWeek (09/06/07), S. Gaudin

The Storm worm botnet that has been pummeling the Internet continuously for the last three months has grown so extensive that it could easily overwhelm the world's top supercomputers, according to security researchers. Estimates of the botnet's size vary, but most researchers concur that it is one of the biggest zombie grids ever observed. MessageLabs researchers spot roughly 2 million discrete computers in the botnet dispatching spam on a daily basis and, after witnessing large spikes in activity, researchers believe the botnet typically runs at roughly 10% of capacity. M. Sergeant of MessageLabs thinks the botnet could involve as many as 50 million computers, but A. Swidler of Postini thinks the botnet is much smaller, though he agrees that it is capable of inflicting great damage. This means that cyber criminals in control of the botnet possess much destructive power and could hurt companies, government agencies, financial centers, or utilities through a denial-of-service (DoS) attack similar to what struck Estonia earlier in 2007. Moreover, the Storm worm botnet has been programmed to launch a distributed DoS attack against computers scanning for malware or vulnerabilities, anti-spam organizations, and even individual researchers attempting to study the

botnet. The botnet authors are making money through pump-and-dump scams and are expanding the botnet with fake news and e-cards spam. L. Baldwin of MyNetWatchman.com calls the situation "scary," noting that the botnet cumulatively sends out billions of messages daily.

Debate Rages Over German Government Spyware Plan
IDG News Service (09/05/07), J. Blau

After passing anti-hacking legislation earlier this year, members of the German government want to permit the development and use of spyware to monitor suspected terrorists. German interior minister W. Schauble has been seeking support for a new security law that would permit federal authorities to secretly investigate suspects' Internet use and stored data by allowing authorities to install Trojans carrying remote forensic software on suspects' hard drives. In February, the German Federal Court of Justice ruled that hacking of computers by police is not permitted under Germany's strict phone-tapping laws and that special legislations would be needed. Schauble says the new security law would only be used in a handful of exceptional cases and on those suspected of planning a terrorist attack, but the proposal has still generated heated debate. Kaspersky Lab virus specialist M. Kalkuhl says the plan undermines the very purpose of security software and that the idea of allowing officials in a country to spy is disturbing. "What's going to prevent police in Germany from breaking into computers in Italy?" Kalkuhl asks. The use of spyware by law enforcement in not new. In the US, the FBI uses a tool called CIPAV that can record IP addresses and send the information to government computers. Meanwhile, Switzerland and Austria are both reportedly considering enacting laws that would allow police to monitor computers online, though neither country has released any official information on their spyware plans.

Personal Data: Up Close and Impersonal
Federal Computer Week (08/27/07), A. Joch

Debate persists between the United States and the European Union regarding how much data to divulge when comparing terrorist watch lists and trans-Atlantic flight manifests. The underlying issue involves balancing the protection of privacy rights with the fight against terrorism, which requires the retrieval of key information. Some computer science experts say that an improved balance might be achieved through data anonymization, a method by which software combs through scrambled data and marks any suspicious patterns. At that point, a government could request a subpoena for records in compliance with the Fourth Amendment. IBM's Anonymous Resolution Technology is used by the US, though not as widely as some experts had anticipated, considering the technology's promise. One key element of IBM's software is one-way encryption, a method for scrambling data without decrypting it, thereby guarding the information from human eyes. However, some security experts caution that anonymization is not a full solution, but rather a first step that must be complemented by a complete security system. As well, some anonymization methods keep encrypted indexes of sensitive data in a central repository, which is a vulnerability, according to computer science professor L. Sweeney, director of the Laboratory for International Data Privacy at Carnegie Mellon University. Sweeney's lab has developed PrivaMix, anonymization algorithms and techniques that have been used for compliance with the Health Insurance Portability and Accountability Act as well as by the Dept. of Housing and Urban Development to protect identities. The software assigns numeric codes to client data and those codes are used when sharing data between networks and over secure Internet connections.

Who Needs Hackers?
New York Times (09/12/07) P. H1; J. Schwartz

Though conceding that computer hackers are a clear threat, experts maintain that some of the most serious and disruptive network problems can be traced to non-malevolent sources, most notably a network's complexity. "We don't need hackers to break the systems because they're falling apart by themselves," says SRI International principal scientist P. Neumann. Nemertes Research's A. Antonopoulos says the transition from relatively simple computing architecttures to massively distributed and connected networks has increased the difficulty of predicting, detecting, and correcting flaws. A problem as simple as a defective network card can have a cascading effect that leads to a network failure, such as the one that shut down computers for the US Customs and Border Protection Agency and delayed flights at Los Angeles International Airport for hours last month. "Most of the problems we have day to day have nothing to do with malice," says Columbia University computer science professor S. Bellovin. "Things break. Complex systems break in complex ways." He notes that it was a cascadeing series of failures that shut down the electrical grid in the Eastern United States and Canada in the summer of 2003. The integration and interdependence of multiple computer networks only makes system-wide vulnerability to a single weak link more likely, according to Veracode CEO M. Moynahan. Johns Hopkins University professor A. Rubin says high-tech voting machines could be extremely susceptible to glitches, and he entertains the possibility that the emphasis on the hacker threat has eclipsed the threat of unintentional problems. One way to minimize non-malicious disruptions is to strengthen systems' capacity for recovery through backup protocols, while Neumann believes the best strategy is to design security and stability into computers from the very beginning.

China's Eye on the Internet
University of California, Davis (09/11/07), A. Fell

Researchers at the University of California, Davis and the University of New Mexico are developing ConceptDoppler, an automated tool that monitors changes in Internet censorship in China. The tool uses mathematical techniques to group words by meaning and identify words that are likely to be blacklisted by the Chinese government. Many countries have some form of Internet censorship, primarily using systems that block specific Web sites or Web addresses, but China's system is unique in that it filters for Web content or specific keywords to selectively block pages, according to UC Davis graduate student E. Barr. The researchers sent messages to Internet addresses in China containing a variety of different words that might be censored. Barr says if China's system was truly a firewall most of the blocking would take place at the border with the rest of the Internet, but some messages passed through several routers before being blocked. A firewall would also block all occurrences of a banned word or phrase, but banned words were able to reach their destination about 28% of the time. By filtering ideas instead of specific Web sites, the system prevents people from using proxy servers or "mirror" Web sites to avoid censorship, but because it is not completely effective the system probably acts more as an unseen watchman, encouraging self-censorship, Barr says. When users in China see a word or phrase that is normally blocked, they might choose to avoid that page, assuming someone is monitoring that site.

EAC to Release Draft Voting-System Guidelines
Government Computer News (09/10/07), W. Jackson

The Election Assistance Commission plans to publish a new draft of guidelines for certifying voting systems in the Federal Register by Sept. 20. Described as a complete rewrite of the

Voluntary Voting System Guidelines adopted in 2005, the new revision bars wireless connections for electronic voting systems, addresses software independence, and updates requirements for a voter-verifiable paper audit trail. The standards are voluntary, but most states use them to certify their e-voting systems. A new set of standards is unlikely to be available in time for the 2008 primary and general elections because the approval process consists of comment periods after two and four months, and the guidelines could be rewritten two times. The National Institute of Standards and Technology assisted the EAC in developing the draft. The commission was created in the wake of the e-voting machine problems of the 2000 presidential election, and was charged with overseeing certification standards.

Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise
Wired News (09/10/07), K. Zetter

Swedish computer security consultant D. Egerstad collected thousands of private email messages from embassies and human rights groups worldwide by simply hosting five Tor exit nodes as a research project. Civil liberties groups, law enforcement, and government agencies use Tor, which is a privacy tool created to thwart tracking of where a Web user goes on the Internet and with whom a user converses. However, many Tor users incorrectly think Tor is an end-to-end encryption device, when in reality Tor has an acknowledged weakness. Tor works by having volunteer-donated servers bounce traffic around as it journeys to its destination, and traffic is encrypted for all but the last leg of the route. When traffic passes through the Tor network's final node, the communication must be decrypted before it can be delivered to its final destination, which means Web activity, instant messages, and email content are potentially disclosed to any Tor server owner who is eavesdropping. The pool of potential eavesdroppers is large, as the Tor network contains some 1,600 nodes, as well as hundreds of thousands of users worldwide. Though the Tor Web site cautions users about the last segment of unencrypted traffic, most users seem to have ignored or missed this warning and have failed to take necessary precautions to safeguard their Web activity, says Egerstad. When Egerstad starting monitoring the traffic through his Tor nodes, he was surprised to find that 95% was unencrypted, and that many embassies and government agencies were using Tor incorrectly. Egerstad also believes this oversight is currently being exploited. S. Nerad, development director for the nonprofit organization that supports Tor, asserts that embassies and other high-risk organizations should be encrypting their data independently.