Taking Snooping Further
New York Times (02/25/06) P. B1; J. Markoff, S. Shane

Officials from the National Security Agency met with a group of venture capitalists to outline their wish list for new data-mining systems that would support and advance the Bush administration's surveillance efforts by better uncovering connections between seemingly unrelated communications. Privacy advocates have vigorously protested the surveillance program, claiming that privacy is violated whether it is a human or a machine that is doing the snooping. Data mining is not a new practice, as insurance and credit card companies have been using it for years to conduct risk assessments and detect fraud, though by applying advanced software analysis tools intelligence agency systems go a step further. Costing up to millions of dollars for an agency-wide deployment in an organization such as the FBI, software tools enable investigators to compile and cross-reference financial data and phone records to look for patterns of suspicious activity. Critics claim that the government has misdirected its surveillance activities, spending vast sums on intercepting the phone calls of American citizens while neglecting to monitor obvious and available resources such as chat rooms frequented by al Qaeda operatives. The Electronic Frontier Foundation has filed a suit against AT&T, alleging that the company's storehouse of phone records and information about Internet messaging, the Daytona system, provides the foundation for the NSA's surveillance, though a company official noted that the system has in place strict access controls. Among the new technologies that the government is developing are a technique to identify the physical location of an IP address and an application that compiles a list of topics by analyzing computer-generated text, while Virage has provided the government with a program that captures up to 95% of the spoken content of television programming, with potential applications for monitoring phone conversations.

Activists Warn of Rerun of Euro Software Patent Fight
IDG News Service (02/27/06), S. Taylor

The Foundation for a Free Information Infrastructure (FFII) has warned that a proposed general patent for the European Union could open the door to software patents. "If you take the case law of the EPO (European Patent Office) and apply it across the board, that means allowing software patents," said FFII President Pieter Hintjens, who described the use of patents in a technology-driven field as "obscene." In the wake of the stalemate over the EU-wide community patent, the European Commission has begun again to solicit input from interest groups and private industry on how to make Europe's system workable. The Business Software Alliance's (BSA) Francisco Mingorance disagrees with Hintjens, however, noting that the consultations are not intended to lead directly to software patents, but rather to address the question more globally, and that the commission's questionnaire suggests more solutions than just the community patent. The questionnaire also offers the options of leaving the system unchanged or modifying the commission through other methods, such as agreeing to cut the number of languages in which patent applications must be filed to three: German, French, and English. Mingorance says the BSA seeks a more transparent and cost-effective patent system, noting that the community patent is unlikely to see ratification after six years

of debate. Hintjens is steadfast in his opposition to a system that makes it easy to obtain junk patents or allows software to be patented.

Cyberthieves Silently Copy as You Type
New York Times (02/27/06) P. A1; T. Zeller

Many computer users are already aware of the dangers of phishing attacks but they may not be aware of the use of keylogging programs that silently copy the keystrokes of computer users and send that information to the criminals. Recently in Brazil, federal police went to Campina Grande and several surrounding states and arrested 55 people for seeding the computers of Brazilians with keyloggers that recorded their typing whenever they visited their banks online. The criminal ring stole about $4.7 million from 200 different accounts at six different banks since it began operations last May, according to the Brazilian authorities. Keylogging programs work by exploiting security flaws and monitor the path that carries data from the keyboard to the other parts of the computer. They are often more intrusive than phishing attacks. The monitoring programs can be hidden inside ordinary software downloads, email attachments, and files. "These Trojans are very selective," says Cristine Hoepers, general manager of Brazil's Computer Emergency Response Team. "They monitor the Web access the victims make, and start recording information only when the user enters the sites of interest to the fraudster." The bad news is that these kinds of crimes are beginning to soar. The amount of Web sites known to be hiding this kind of malicious code nearly doubled between November and December to more than 1,900, according to the Anti-Phishing Working Group. Last year iDefense says there were over 6,000 different keylogger variants, a 65% increase from 2004. The SANS Institute estimates that last fall, as many as 9.9 million machines in the United States were infected with some kind of keylogger, putting as much as $24 billion in bank account assets in the hands of crooks. To reduce the growing threats, the Federal Deposit Insurance Corporation strengthened its guidelines for Internet banking this past fall, to require banks to do more than just ask for a user name and password.