privacy news

Workplace Privacy

Workers disciplined over E-mail, Internet abuse

A September 4 report by the online news report I.T. notes that the Australian subsidiary of Siemens has disciplined a number of employees after an internal review of Internet and e-mail use.

The company released a statement saying that as part of its audit plan, a regular review of Internet and e-mail use had revealed "a number of employees who have severely breached policies governing use of the Internet and e-mail systems at Siemens Ltd". One employee was dismissed and several others were severely reprimanded.

For further information visit: www.it.mycareer.com.au/breaking/2001/09/04/FFXPCQ1L6RC.html

US Judge calls for review of employer access to employee computers

Just months before the action by Siemens against its employees, an American judge challenged the new "legal principle" of employer access rights to employee computers. The principle suggests that if a corporation, business, or government entity owns a computer, and if an employee puts personal matter onto that computer, the author has neither a right nor an expectation of privacy in the computer-stored material. James M. Rosenbaum, chief judge of the United States District Court for the District of Minnesota, argues that the legal principle seems to have sprung forth spontaneously:

"There is, however, little evidence that it was inscribed on tablets or received atop a mountain. It seems to me, like many a *priori* truths, it ought to be further examined. This examination is essential, because a free society has a vital interest in preserving for its citizens a central core of privacy to protect their most personal thoughts. If this new principle is erroneous, the error is pernicious."

Judge Rosenbaum argues that the present regime, which gives employers a "near-Orwellian power to spy and snoop into the lives of their employees," is not tenable. The use of an employer's computer should not be equated with the loss of its operator's rights. A society which values individual freedom cannot function this way, says Rosenbaum.

Citing history as an ally, Rosenbaum reminded his readers that in the years leading to the Revolutionary War, the British used general searches as a way to root out anti-English traitors and sympathizers. "The citizens of the nascent Republic found these searches wholly unreasonable."

To respect both employers' and employees' rights, Judge Rosenbaum proposed a "cyber time-out," coupled with reasonable notice to the worker. An employer with a definable reason to examine an employee's personal computer ought to be permitted to do so. But prior to undertaking its examination, the employer ought to give the employee reasonable notice of its concerns.

A reasonable time-out might be 72 hours. Failing to give the required notice, or violating the time-out, should bar the employer from taking any adverse employment action against the employee. If the employer failed to comply, the employee would be able seek damages resulting from the failure.

The complete article by Judge Rosenbaum can be found at: www.greenbag.org. The legal citation for his article is 4 Green Bag 2d 169 (2001).

Computer and Other Security Issues

Virus transmits computer files to outsiders; corporate security prevents virus spread

Antivirus experts said that the SirCam worm virus that emerged in mid-July may pale in comparison to other viruses, but that it has the potential to release sensitive information stored in infected computers. To its chagrin, the FBI found this out in late July.

SirCam was the No. 1 virus at antivirus-software maker McAfee, with 144,000 infections reported in one day in late July.

The *New York Times* reported on July 24th, 2001, that a major part of the reason the worm has stayed below epidemic status is that the most fertile breeding grounds for a worm – large corporate e-mail systems – are for the most part equipped with security filters that reject infected messages.

The SirCam worm spreads by e-mailing copies of itself to everyone in the infected computer's Windows address book. It also sends itself to any e-mail addresses contained in the Web browser's cache files, which store recently viewed pages.

The virus poses a particular privacy problem. SirCam sends a randomly chosen file from the infected computer's hard drive, potentially sending confidential business data or embarrassing personal information along with itself. In late July, a researcher at the FBI's National Infrastructure Protection Center – the bureau's "cyberprotection unit"

– allowed the SirCam worm to send private FBI documents from a bureau computer to outsiders, according to an FBI statement.

Computer security advisers have suggested that consumers need to have better protection both on their PC and or whatever networks the computer attaches itself. As well, consumers should probably speak with their Internet Service Provider (ISP) and ask why it is not blocking such infected messages.

Meanwhile, in late August, House Government Management and Information Technology Subcommittee Chairman Steven, R-Calif., organized a hearing to assess steps federal agencies can take to evade threats posed by Code Red, SirCam and other malicious viruses.

For further information about the hearings, see: www.newsbytes.com/news/01/169606.html

Credit Card Security and E-Commerce

Reuters reported on August 16 that credit card crime has become a $2 billion global problem. It based its conclusion on a report by business information group Datamonitor, "Combating card fraud."

Datamonitor reported a 65 percent average increase in card fraud in Germany, Spain, Britain, Italy and France in 2000. U.K. credit card crime virtually doubled from the previous year. Reuters called the UK the "fraud black spot" at an estimated $428 million.

Still, the fraud rate in Europe is relatively low, at 0.06 percent; fewer than one in 1,500 transactions is fraudulent. The figure for the U.S. is one in 2,500.

The Datamonitor report suggested that Europe's anti-fraud technology, such as the microchips that can store security codes, address data and possibly even fingerprint scans or voice recognition data, will give business the upper hand.

The UK Association for Payment Clearing Services (APACS), a non-statutory association of major banks and building societies and the umbrella body at the centre of the UK payments industry, has published a report, "Card Fraud: The Facts 2001". One issue it discusses is card fraud over the Internet. The Association states that the incidence of hackers stealing cardholder data from websites is very low compared to other ways criminals access card details. However, there have been some incidents. The solution? "In the long-term," says the Association, "it is chip cards that will play a pivotal role in providing the base for secure e-commerce."

For further information visit: www.uk.biz.yahoo.com/010828/66/c2d05.html, www.cardwatch.org.uk/, www.news.cnet.com/news/0-1007-200-6893015.html, www.siliconvalley.com/docs/news/reuters_wire/1414066l.htm.

Microsoft's new operating system, Windows XP, raises privacy concerns

The *New York Times* (September 6th 2001) reports that Microsoft's soon-to-be-released operating system raises privacy questions "at every turn:"

"During installation [of the operating system], you're first asked if you're ready to "activate" your copy of XP (send information about your PC's configuration to Microsoft), and then if you'd like to register it (send your address and phone number to Microsoft). If you try to use the Windows Messenger program, you're told you must sign up for a Passport (send your e-mail address, city and ZIP code to Microsoft)."

Says the author of the article, "it's easy to be alarmed by the notion that a single company's database may soon list 90 percent of the world's computers."

State Powers

FBI monitors keystrokes to circumvent suspect's use of encryption

FBI investigators tackling a sophisticated suspect for illegal gambling and loan-sharking have raised the hackles of privacy advocates who are concerned about the government's ability to conduct surveillance of personal computers. In its attempt to circumvent the encryption software used by the suspect, the FBI employed a technique known as "key-logging."

Earlier in the investigation, FBI agents had entered the suspect's office with a search warrant and copied his computer files. One file was encrypted with a program called PGP – Pretty Good Privacy. Because they were unable to crack the encryption code without a password, agents went back again with a search warrant and placed the key-logging device on his computer. They monitored the computer for about two months. The surveillance ultimately produced the password – nds09813-050. A source close to the case confirmed that the password was the prison identification number of the man's father.

The *Washington Post* reports that the man's defence team and privacy organizations are trying to force the government to reveal how the "key-logging" technology works as a possible prelude to asking that the evidence it yielded be thrown out. The government is vigorously opposing disclosure.

Privacy advocates are especially concerned that the key logger was planted on the basis of a simple search warrant and not a court-approved wiretap order, which is more difficult to obtain and carries far greater restrictions. In an interview with the BBC World Service, David Sobel, of the Washington-based Electronic Privacy Information Center (EPIC), said: "I think it has significant implications for future law enforcement investigations. It's the idea of secret government surveillance technology being installed with very little oversight or accountability."

Further information visit: www.epic.org/crypto/scarfo.html.

Australian Police officers convicted of disclosing information from Police computers

Two former Victoria police officers were convicted and fined AUS$2,000 for illegally disclosing private

information from the force's computer system.

The prosecutor suggested that the cases against the two officers were not isolated, and that other prosecutions of police officers would likely occur. He noted that police had free access to and were trusted with the Legal Enforcement Assistance Program computer, which contained a large amount of private information.

One police officer acted as an unlicensed private inquiry agent by agreement with the other, who ran a company investigating car accidents.

For further information visit: www.it.mycareer.com.au/breaking/2001/09/04/FFX55Y0L6RC.html

Netherlands Commission recommends easier access to personal data for law enforcement

A commission recommended last week that Dutch police be able to gain access to all client information in company databases. The minister of Justice said he would adopt the proposals in new legislation.

The commission, led by Professor P. Mevis, concluded that current investigative powers no longer satisfy police needs in an information society. Privacy rules are often an obstacle, as are legal definitions that do not reflect technological development. And companies do not know their obligations – in many cases voluntarily providing confidential client information. The commission considers the situation unacceptable for both parties.

The commission proposes that police officers be able – without a legal order – to ask for such personal information as name, address, client number, bank account number, access codes, and registration plate. And the personal information need not concern only suspects. Police would be authorised to seek information about a group of persons to investigate networks and communications, and movement of money or goods. This is pro-active investigation – police screening whole groups of citizens to identify criminal patterns.

The organizations required to cooperate with police runs the gamut from telephone companies to educational institutes, and Internet providers to hospitals. Police would still require a legal order by the public prosecutor when seeking "location data"; for example, credit card and telephone bills, supermarket bonus card records and banking transactions that can establish the whereabouts of persons or goods. Even "sensitive information" about political beliefs, race, health, sexual habits or membership in trade unions, can be demanded when there is a serious breach of the legal order.

The commission further proposes giving police the power to ask for 'future data', so companies will be obliged to continue providing all new information.

The commission and the Minister of Justice maintain that the proposals strike a 'fair balance' between the needs of law enforcement authorities, organizations and privacy. Civil liberties groups argue the proposals reflect only police wishes.

'The law enforcement authorities drew up their list of presents and they got them all. This proposals means a huge increase in the power of police, with little or no means of control,'' commented Bits of Freedom.

South Africa: Concern About Security Service Powers to Snoop

The BBC reported on August 13th that protests are growing in South Africa against the country's plan to give the security services new powers to monitor terrorists and serious criminals. The Interception and Monitoring Bill was passed by South Africa's Cabinet in July. It is now due to go before Parliament.

The bill provides for state monitoring of all telecommunications systems, including mobile phones, internet and e-mail, once permission has been granted by relevant authorities. The bill allows for monitoring to take place where there is a "threat or alleged threat to the security or other compelling national interests of the Republic." In most cases, says the BBC, a judge must grant the order, but in some instances a police or army officer of a particular rank may do so.

Some media organisations are now criticising the legislation as a threat to the constitutional right to privacy and freedom of speech.

Telecommunications service providers must bear the cost of supplying the necessary technology for state monitoring and interception. If they fail to do so within three months, they face significant fines.

One provider of mobile phone services stated that the "constitutional right to privacy of our customers is sacrosanct and we will only allow interception if the correct legislative procedures are followed."

For more information visit: www.bday.co.za/bday/content/direct/1,3523,904405-6099-0,00.html, www.news.bbc.co.uk/low/english/world/africa/newsid_1484000/1484698.stm

Health Information

Technological barriers to genetic information collapsing?

To date, the scientific complexity of deciphering the human genome has helped to limit threats to genetic privacy. However the *Economist* magazine reports in its June 23rd 2001 edition that a new gene sequencing technique being explored in the United States could decode a person's genome in hours instead of years. Refining the technique could take up to a decade. "But," says The Economist, "the prize – anyone's genome, on demand, within hours – seems well worth the wait."

UN special session on HIV/AIDS cites need to respect confidentiality and privacy

The first UN General Assembly Special Session (UNGASS) on HIV/AIDS, held in New York in late June, has strongly endorsed the need to protect the confidentiality of personal information about HIV status. This was necessary to prevent

discrimination and to allow the realization of the human rights of individuals with HIV/AIDS. This included access to employment, health care and social services. In an extensive declaration issued at the end of the special session, the General Assembly declared its commitment to privacy and confidentiality in relation to HIV/AIDS:

By 2003, enact, strengthen or enforce as appropriate legislation, regulations and other measures to eliminate all forms of discrimination against, and to ensure the full enjoyment of all human rights and fundamental freedoms by people living with HIV/AIDS and members of vulnerable groups; in particular to ensure their access to, *inter alia* education, inheritance, employment, health care, social and health services, prevention, support, treatment, information and legal protection, while respecting their privacy and confidentiality; and develop strategies to combat stigma and social exclusion connected with the epidemic.

The preamble to the Declaration noted that lack of confidentiality undermines prevention, care and treatment efforts and increases the impact of the epidemic on individuals, families, communities and nations.

For further information visit: www.hdnet.org.

Internet Privacy

Gallup Poll reveals concern about Internet Privacy

The Gallup Organization recently released the results of its June 2001 online survey of email users on Internet privacy. Gallup reported that nearly eight in 10 e-mail users are at least somewhat concerned about the privacy of personal information that they give out on the Internet. However, just 28% were "very concerned." The poll was conducted via the Internet between June 14-26. E-mail users were most worried about misuse of credit card information and felt least comfortable giving out their social security number and credit card numbers online. Eight out of 10 respondents said they were very concerned or somewhat concerned about the misuse of credit card information given out over the Internet.

In contrast, only four of 10 were very concerned or somewhat concerned about their business or company monitoring their e-mail and Internet usage.

Two-thirds of respondents thought that the US federal government should pass more laws to ensure citizens' privacy online, while 33% thought the current laws were sufficient.

For further information visit: www.gallup.com/poll/releases/pr010628.asp.

CBI supports amendments to proposed EU Telecoms Data Protection Directive

The Confederation of British Industry maintains that the proposed EU Telecoms Data Protection directive is premature, since the full impact of the 1995 Data Protection Directive had not yet materialized. Even so, in its June 15th 2001 Brussels Update, the CBI welcomed the European Parliament's suggested amendments to the Telecoms directive. The amendments related to traffic data retention. Traffic data include the times of ISPs logging in and out, names of web sites visited, and the size, headers and destination and e-mails sent.

The CBI report noted the initial moves to force Communication Service Providers (CSPs) to retain traffic data of all users for several years so that the data could be made available to law enforcement and intelligence agencies.

The CBI argued that the proposed amendments would give traffic data the same confidentiality as the content of communications. The CBI reported that it had sent comments to MEPs urging them to support the amendments.

At the same time, European ISPs and Data Protection Commissioners have increased their opposition to possible access by police agencies to electronic communications.

For further details about this opposition see: www.thestandard.com/article/0,1902,27121,00.html

European Parliament approves e-coms networks and services proposal

On June 13th 2001, the European Parliament approved by a large majority a proposal on electronic communications networks and services. The goal of the proposal is to update existing measures on universal service and set out specific rights for users. Together with a number of amendments, the directive forms part of the "telecommunications package" designed to open up the telecoms market to greater competition.

On the issue of data security, Parliament encouraged providers to ensure that their own services are secure. In relation to the European emergency number '112', Parliament agreed in principle with the Commission's proposal that companies operating public telephone networks should make caller location information available to authorities handling emergency calls. However, Parliament stressed that this provision must not compromise data protection or civil liberties. Compliance with the directive on personal data protection in electronic communications was essential.

For further information, contact e-mail: lega-press@europarl.eu.int

EC launches site to fight child porn and cyber crime

The European Commission has launched a website aimed at protecting children against paedophiles, cyber crime and racism on the Internet.

The "Awareness Exchange" website, www.saferinternet.org, was launched as part of the EC's "action plan" to fight illegal content and activities online. It contains information on building hotlines to encourage self regulation, developing effective filtering and rating systems,

encouraging awareness, news stories from the EC and beyond, as well as resources and advice. The site also has links to organizations seeking EC funding for initiatives to fight online fraud.

While clearly the site's central focus is on efforts to mould European laws and regulations, there are international links and the information and discussion is relevant for visitors from outside the EC.

Spanish fears of a website inquisition

The Spanish government's proposal to regulate Internet activity is meeting stiff opposition from civil libertarians who say the measure would hamper free speech. The Law of Information Society Services and Electronic Commerce (LSSI) would force websites to register with the government and require Web hosting companies to police content by reporting suspected illicit activity.

According to Luis Fajardo López, a law professor at the University of Gerona, government agencies could also shut down websites and seize their content and activity logs to combat crime. But he argues that a website's archives can be altered by anyone and thus cannot be used to incriminate anyone. Carlos Sánchez Almeida, a Barcelona attorney who specializes in Internet law suggested the measure would violate Spain's constitutionally protected free speech by allowing the government to seize Internet content it considers offensive.

Kriptopolis, a cryptography website, has launched an aggressive campaign against the legislation. Sympathizers have flooded the inboxes of the Ministry of Science and Technology (the bill's sponsors) with protests. The ministry concedes that the measure is a rough draft that needs work.

Online banking fails to make the privacy grade in US

A study released on August 29th by the US-based Center for Democracy and Technology concludes that online banks are not giving consumers convenient, online opportunities to limit disclosure of their personal financial information. This forces customers to use more cumbersome offline mechanisms to opt-out of data sharing.

The study found that, of 100 banks studied that offer their customers the ability to open accounts online and use other banking services online (such as bill payment and mortgage quotes), only 22% provide customers equally convenient online means of preventing information sharing with other companies. The Center stated that its greatest concern was that several mortgage companies offering online services were not giving their customers any notice of their privacy practices. This, the Center suggested, seems to be in direct violation of the new federal banking law, the Gramm-Leach-Bliley Act ("GLB"), which went into effect on July 1st.

Among its recommendations, the Center called for financial institutions to follow the best practices identified in the study. It also recommended that the Federal Trade Commission look into the practices of the online mortgage companies that do not give consumers notice of their privacy practices. The FTC has oversight responsibility under the GLB law for various institutions, including the independent mortgage companies. These companies fared worst in the study.

On the same day that it released its study, the Center filed a complaint with the Federal Trade Commission about five online mortgage companies that did not respond to the Center's request to post a privacy policy on their web sites.

For further information see www.cdt.org/publications/pp_7.07.shtml#1, www.newsbytes.com/news/01/169478.html.

Privacy Policy/Management

Canadian gun licence applications overly intrusive

Questions on Canada's gun licence application forms about marital problems, divorce, suicide and alcohol abuse are overly intrusive and should be eliminated says federal Privacy Commissioner, George Radwanski. The forms are part of a rigorous screening process gun owners must undergo before being given a permit to own a weapon and buy ammunition.

Mr. Radwanski's office reviewed the questions, as well as the research and evidence on which the Department of Justice relied to draft the forms, and concluded that the department had failed to prove that the answers could predict violent behaviour. According to his report, the firearms centre already has information about any violent and dangerous behaviour from exhaustive searches of criminal and police records now required before applications are approved.

Opponents of the licensing process say the report vindicates their stance against the personal history questions. Gun control advocates are appalled, pointing to extensive research on suicide and violence, homicide inquest reports and the advice of public safety experts. According to one academic who advised the department during development of the Privacy Act, they considered it specifically, as well as the need for the particular information.

Mr. Radwanski also recommended tighter controls on volunteer verifiers who handle sensitive personal information, and questioned the need to gather information from credit bureaux.

The Canadian Firearms Centre says it will consider the report.

Ontario Information and Privacy Commissioner announces release of privacy diagnostic tool

Ontario Information and Privacy Commissioner Dr. Ann Cavoukian has announced the the release of a new privacy tool – the Privacy Diagnostic Tool (PDT). The PDT was developed by Dr. Cavoukian's office with the assistance of private sector security and privacy advisers.

The Commissioner states that PDT will help businesses to determine their state of privacy readiness, and how to improve areas identified as being less than sufficient.

Using a question and answer format, the PDT takes businesses through 10 international fair information practices, including accountability, consent, accuracy, safeguards and openness. Businesses are informed about the objectives of each principle and are alerted to the risks they may face if they fail to comply. The self-assessment tool provides a quick, initial gauge of a business's privacy status quo.

The PDT is available in workbook form, or as an electronic tool that can be downloaded, completed, and used to generate reports about next steps, at www.ipc.on.ca/english/resources/resources.htm.

---

continued from page 5

information society. As part of that policy, specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information. A Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies must be established.

On September 5th 2001, the European Parliament accepted the report and its recommendations in a 367-159 vote.

For further information on the report see www.europarl.eu.int/committees/echelon_home.htm.

continued from page 16

There are various self-regulatory schemes that seek to regulate the use of data for marketing purposes. Examples include the Direct Marketing Association, which has a privacy promise and the Network Advertising Initiative.

In conclusion, privacy has become a major domestic concern in the United States. In a recent privacy poll conducted by the Wall Street Journal, privacy was the major concern of those responding to the poll (ahead of World War III, famine, over-population, global warming, etc.). This, together with technological developments such as personalised marketing on the Internet, make it inevitable that marketing will be regulated.