ISSN. 1363-6650

APRIL 1998
Issue 16

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing

Third Floor, Colonnade House,
High Street, Worthing,
West Sussex, UK
BN11 1NZ

Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail:ijfc@pavilion.co.uk
http://www.forensic-computing.com

Comment

Imagine the scenario - after weeks of tireless and dedicated work the detective has successfully traced a hardened and dangerous computer hacker and has made an arrest. Using the best technology available he has copied the suspect's machine for evidential purposes and, after several hours of tough interviews, he has finally got a confession from the hacker.

It seems pretty much cut and dry. But in reality that's a long way from the truth and the suspect could still walk free.

The whole point about forensic computing, like any other branch of forensics, is that the whole investigation, from start to finish, has to stand up in a court of law.

This means following strict procedures and methods to prove that the evidence is really what it claims to be, and has not been falsified or contaminated in any way whatsoever.

Methodology and standard practise are gradually being built up and assembled in police forces across the world, which has to be a positive step, although this is still pretty much at a very early stage.

The real trouble comes when the evidence is presented in a law court. Often the laws under which the computer crimes are prosecuted have not been fully tested, leaving large areas for misinterpretation or confusion, particularly if the judiciary or juries are not themselves computer literate.

And then into this turbulent mix the defence lawyer, whose job it is to get the hacker or Internet paedophile off the hook, will attempt to argue the inadmissibility or inconclusiveness of just about every piece of evidence.

Often in the Journal news stories start with the phrase "In the first case of its kind..." and this is typical of just about every country that is investigating computer crime. This is a science in its infancy and correspondingly the law surrounding it are being developed alongside.

It is only by test cases, precedent, argument and maybe even losing a few fights that both law enforcement agencies and the prosecuting services will understand each others needs and come up with a comprehensive solution.

In this issue of the Journal we have two excellent articles covering the problems of presenting evidence in court. The first, Inadmissible evidence? looks at the issue of contamination, both accidental and deliberate, and asks how this can be minimised or at least determined and exposed.

The second piece is a thorough look at the part of the UK Police and Criminal Evidence Act which covers computer generated evidence. The author's central message is that computer evidence is not vastly different from any other sort of evidence, and that if the courts are to pick holes then the law has to give a clear message to law enforcement on just how evidence is to be handled.

Each country has different cultural and legal backgrounds and will take a different approach to computer forensics, but the goals are the same everywhere - the successful investigation and prosecution of criminals who use technology in whatever way.

It will take many years before everyone in law enforcement and prosecution is able to deal with computer crimes as routinely as any other offence, but that day will come.

News

Computer crime booming says study

A report by a security group in the US says technology offences are growing alarmingly, with a large rise in the number of external hacking attacks.

San Francisco's Computer Security Institute, a professional association for security personnel, described the "wired world" as becoming "increasingly dangerous" in 1997, with breaches up in all categories compared to previous years.

Patrice Rapalus, CSI's director, said technology wouldn't fix the situation because it is not entirely a technological problem. She said:"I think a greater emphasis should be placed on educating and training computer users to safeguard the information they see. Technology plays a vital role, but it's not the only component in computer security."

The survey findings were released in the third annual Computer Crime and Security Survey in the US. CSI conducts the study annually with the US FBI to examine the extent of computer crime to make the public more aware of it.

The 520 surveyed "security practitioners," as CSI calls them, mostly work for US corporations, government agencies, financial institutions, and universities. CSI says nearly two-thirds of the respondents said their organisations had suffered security breaches in 1997, up 16 per cent over the previous year.

And nearly three-quarters said breaches had cost money, with reported losses of $136.8 million, an increase of 36 per cent.

The FBI says this amount is only a fraction of the real loss because many companies still do not report security breaches, fearing breaches would look bad to investors and the public.

Among breaches that did get reported, 44 per cent of respondents said their companies' own employees made the attacks. Other serious breaches included denial of service attacks (25 per cent), outside penetrations (24 per cent), theft of proprietary information (18 per cent), financial fraud (15 per cent), and data or network sabotage (14 per cent).

The most serious losses still come from large-scale insider crimes with about $50.6 million or 40 per cent of the total $136.8 million being reported by only 18 respondents.

Another 20 respondents reported $33.5 million lost to theft of proprietary information, 32 reported $17.3 million lost to telecommunications fraud, while 29 respondents reported $11.2 million in losses to computer-related financial fraud. In the area of increased outside attacks, Internet connections were named as a source of serious attack by 54 per cent of the respondents, up from 47 per cent the year before and 37 per cent in the baseline 1996 study.

CSI's Rapalus said the results show companies "may think that they are spending the requisite amount" on security but "the dramatic increase in quantified dollar losses indicates otherwise."

Details on the study can be found on the Internet at http://www.gocsi.com

Hackers hit Windows NT systems in attack

Hackers hit thousands of computer users with an assault on Microsoft's Windows NT operating system that shut down systems for a short time.

The affected users were mostly on government and educational systems where networks were directly connected to the Internet, without upgrades that would have safeguarded the computers.

Windows NT is a popular operating system for large users of computers. The attacks, which appeared to be automated, caused computers to crash, but there were no reports of any computer data being lost or stolen, said Ed Muth, who manages Microsoft security.

Muth said: "Even though the practical implications of this are relatively modest, this is not a matter that should be taken lightly by customers, by the industry or by law enforcement agencies."

He urged users to download fixes to prevent further attacks. "It's important that people invest the effort to do the right thing," he said, noting that protected systems weren't hit.

The unknown culprit or culprits attacked Windows NT systems by sending a barrage of invalid data to computers. The assaulted computer then devotes increasing amounts of memory and processing power to the invalid data until it crashes.

Karan Khanna, product manager for Microsoft's Windows NT Server Team, said: "If you have a completely updated system this attack would not be possible. The problem is some network administrators are slow in getting the latest patches we post on our Web site."

Servers affected by the malicious activity included Web operations at Massachusetts Institute of Technology, Northwestern University, the University of Minnesota, Ames Research Centre, Carnegie Mellon University, the US Navy (unclassified servers), and University of California campuses in Berkeley, Irvine, Los Angeles, and San Diego.

NASA Headquarters in Washington as well as 12 other NASA sites across the country were also affected.

Considered at this time as a malicious prank, the series of events was accomplished by instructing a server to devote excessive memory resources to solve a problem that can't be solved. The outcome is each server freezes or "hangs" and must be rebooted. There were no reports of data theft or damage to files.

According to Khanna, the attacks did not occur simultaneously, but rather as a chain or series of crashes. The attack was not successfully traced.

E-mail fraud

New York State's Attorney General Dennis Vacco has vowed to clamp down on fraudsters who use technology to try to dupe others.

Vacco, already head of a nationwide taskforce to quash online child porn, has set his sights on also cleaning up the fraudulent "get rich quick" and illegal pyramid schemes over the Internet.

The Attorney General has set in motion a long-planned crackdown on illegal e-mail activity, announcing settlement agreements in 12 cases involving participants in illegal pyramid schemes circulated on the Net.

"This is an important milestone in our common efforts to make the Internet a safer and more enjoyable environment for millions of e-mail users," Vacco said

in announcing the agreements. "As the chief law enforcement officer in New York, I am committed to making sure that criminal activity conducted over the Internet is investigated and prosecuted."

Vacco's fraudulent e-mail crackdown is part of an overall Internet strategy the Attorney General started last October with a cyber crime "tip line." The tip line puts users in direct contact with the Attorney General's Internet Unit to alert the office of suspected fraud or criminal activity on the Web.

The tip line can be accessed from Vacco's home page at http://www.oag.state.ny.us

FBI warns Congress

Hacking into computer networks is reaching epidemic proportions, causing hundreds of millions of dollars in business losses and untold threats to national security, the FBI told Congress.

Speaking before the Congressional Joint Economic Committee, FBI Deputy Assistant Director Michael Vatis said that the Internet and other advances in information technology "go well beyond the potential loss to the individual victim," affecting "our national economy and, indeed, our national security."

Vatis, who also is chief of the FBI's recently established National Infrastructure Protection Centre, that a 1996 Defence Information Systems Agency study estimated that as many as 250,000 attacks may have occurred on Defence Department systems in 1995 alone.

He said: "The reliance on new technologies comes with a price, and that price is a new vulnerability to those who would cause harm."

Vatis said the nation's infrastructures are particularly vulnerable, since they are increasingly interdependent and interconnected with one another.

"The banking system depends on the availability and reliability of the telecommunications systems and the Internet, which in turn rely on electrical power," Vatis said. "And our transportation system depends on the availability of gas and oil supplies, which in turn are controlled through the use of new information technologies."

Vatis said pending investigations into computer system intrusions by the FBI have more than doubled in the last year, increasing 133 per cent from 206 to 480 in fiscal year 1997.

And although there was a corresponding 110 per cent increase in information and indictments from 10 to 21, a 950 per cent increase in arrests from 4 to 42 and an 88 per cent increase in convictions from 16 to 30, Vatis warned that these numbers represent only the tip of the hacking iceberg.

He said that while the most imminent threat today comes from insiders, such as disgruntled employees, recreational hackers are becoming increasingly dangerous as well.

With recreational hackers, Vatis said the "problem is exacerbated by our continued romanticisation of hackers as technical whizzes who are really not doing anything wrong but are actually providing a service by pointing out the vulnerabilities in a system."

"But do we praise a burglar for demonstrating the vulnerability of our home security by breaking in and stealing," Vatis asked. "Of course not."

He added: "Our society has to do a better job of educating children and young adults that breaking into someone else's computer system has serious consequences, and is a serious crime.

"Although we have not experienced the electronic equivalent of a Pearl Harbour or Oklahoma City, as some have foretold, the statistics and our cases demonstrate our dangerous vulnerabilities to cyber attacks."

- FBI director Louis Freeh told a Senate hearing that parental supervision was the most important weapon in the fight against online computer pornography. Freeh, testifying before the Senate Appropriations Committee's commerce, justice, state, and the judiciary subcommittee, cautioned that unless parents were aware of the dangers of unsupervised Internet activity, their children could become targets.

"Any contact with a voice on the Internet is unknown contact," Freeh said. "You don't know who you're speaking to because anybody can be anybody on the Internet."

Agreeing that education in safe Internet use was necessary in combating online child pornography, FBI agent Linda Hooper called parental supervision of Internet use "most important."

Hooper, in charge of the FBI's Baltimore, Maryland field office, told the subcommittee that one agent posing as a teenage girl found that the other 22 persons in a teen chat room turned out to be adults with dubious intentions.

The program to fight child pornography, started in 1995, already has led to 161 arrests and 184 convictions, Freeh said, and helped fund 60 positions, including 25 agents. The program, based in the Baltimore field office, plans to start a second unit, Freeh said.

Net theft lawsuit

An agreement has been reached in a copyright infringement lawsuit in the US involving material on the Internet.

Software Publishers Association has reached a settlement in a civil copyright infringement lawsuit involving the Internet. The complaint alleged the defendant was reproducing and distributing copyrighted software and related infringing materials, such as serial numbers and cracker tools, over the Internet without prior authorisation.

The defendant, Robert F. DePew of Erie, Pennsylvania, agreed to refrain from any further infringements and stipulated to a damages award of $180,000, Peter Beruk, SPA's director, North American anti-piracy, said.

According to Beruk, DePew, using such Internet sites as http://www.velocity.net/~overlord , provided an extensive list of serial numbers for about 4,500 software products, some of which retail for thousands of dollars.

DePew also provided cracker tools that are used to circumvent the copyright protection mechanisms in software, Beruk said. In addition, a number of software programs were available free for download, and "more than 53,000 people visited the sites before they were taken down, gaining access to the infringing software and materials being offered," he said.

Beruk said the suit against DePew, filed in the US District Court for the Western District of Pennsylvania, came

after an exhaustive seven-month investigation tracking each site and monitoring the alleged infringing material on each site.

In addition, SPA hired a computer expert to testify to the illegality of the distribution of serial numbers and cracker tools. The plaintiffs in the suit were Adobe Systems, Autodesk, Claris, Corel, Intuit, Macromedia and Visio.

Beruk added that as a result of the newly enacted No Electronic Theft Act, signed into law on December 16, 1997, Internet pirates may face criminal prosecution for the unauthorised distribution of software and related infringing material, in addition to civil penalties.

- A federal operation has resulted in the arrested of a man suspected of replicating, advertising and selling counterfeit software in the US.

The arrest came two weeks after the man, 27, from San Diego, California, received a "cease and desist" letter from the Software Publishers Association.

Rudy Orjales, SPA's anti-piracy counsel, said the association was notified of the successful sting by a detective from the San Diego Police Department's Regional Fraud Task Force after the task force received a delivery of several hundred counterfeit copies of Microsoft Office Pro 97.

Evidence recovered during searches of the man's vehicle and home included sales, counterfeit CD-ROMS, a CD-ROM writer and customer lists. He had advertised copies of Microsoft Office Pro 97 and other programs for $40 per copy.

Orjales said the federal task force that conducted the sting is a combined effort by local, state and federal law enforcement agencies. The task force is headed by the US Secret Service due to its jurisdiction over cases involving electronic access devices.

Net privacy summit

The White House has announced plans for a summit covering Internet privacy concerns.

The proposed meeting, currently scheduled for May, would follow the outline of last December's three-day Internet online summit focusing on children's issues led by Vice President Al Gore and Attorney General Janet Reno.

According to Under Secretary of Commerce David Aaron, the meeting, which would bring together government, industry and privacy rights leaders, would re-examine the Clinton Administration's current policy to follow the online industry's self-regulatory guidelines regarding online data collection.

During last December's summit, the Federal Trade Commission released a study showing that more than eight out of ten children's Web sites visited by the FTC collected identifiable information - most without seeking permission.

David Medine, associate director for credit practices at the FTC said: "Surveys have shown that increasing numbers of consumers are concerned about how their personal information is used in the electronic marketplace."

Online bookies charged

Federal authorities in the US have vowed to fight illegal Internet gambling, with the arrest of 14 owners and managers of six betting companies.

US Attorney Mary Jo White said: "Such blatant and widespread efforts to evade gambling laws cannot and will not be tolerated. These cases send an important message that we will vigorously prosecute any use of the Internet to conduct criminal activity.".

The cases will become the test bed for laws against Internet gambling.

White added: "Federal law clearly prohibits anyone engaged in the business of betting or wagering from using interstate and international wire communications, including the Internet and telephones, in connection with betting on sports events."

Underscoring the importance the Justice Department is putting on these cases, US Attorney General Janet Reno told Internet betting operators that "we have a simple message: you can't hide online and you can't hide offshore."

The six separate complaints charge the defendants, all of whom are US citizens, but run Internet sports betting operations headquartered in the Caribbean and Central America, with conspiracy to transmit bets and wagers on sporting events via the Internet and telephones.

All of the companies advertise and promote their sports betting operations to US customers on Web sites on the Internet, according to the complaint.

The defendants also solicit US bettors by, among other things, maintaining marketing offices in the US, advertising in magazines published and distributed in the US, and mailing promotional literature from locations in the US, the Justice Department charged.

Each of the defendants faces a maximum sentence of five years in prison and a fine of up to $250,000 if convicted, White said.

Touch Tone America Inc. said Monday its chief executive officer Kerry Rogers was one of the 14 people charged.

Rogers denied the charges, saying he was merely hired by Winner's Way, one of the alleged betting operations, to create a Web site. He said: "These charges are uneducated, misguided and quite frankly I don't think the government has a clue about how the Internet works."

- Meanwhile, the state of Queensland in Australia has introduced legislation, which will licence and regulate Internet-based casinos and other online betting operations.

The new legislation is being pitched as protection for online punters. Under the legislation, to be administered by Queensland's Office of Gaming, potential online gaming operators will be subject to the same checks as physical casinos. The new laws will prohibit underage betting and credit betting online. Punters will have to register with an online gambling outfit and satisfy a 100-point identity test, similar to opening a bank account.

"Peace treaty" for hackers

A group of hackers who call themselves The Enforcers have pledged to end a series of Web site attacks.

The group hit the headlines recently when two of its members were among three hackers implicated in attacks on

military computer networks.

"We, the Enforcers, have decided that it would be in the best interest of the hacking community and the security community at large to cease and desist all web site hacking of external businesses," the group wrote on its Web site.

"We agree that our actions are not productive and are doing more harm than good towards the security community. As an agent of the Enforcers, I hereby state that all Web site hacks on external sites will be immediately halted."

Members of the group said they had been attacking Web sites in retaliation for the arrest of members and the sullying of their names, who were fighting online pornography and not attacking military computers, they claimed.

The Enforcers group said it was more interested in the fight against child pornography and anti-Semitic speech than hacking military servers and its Web site urged Net surfers to contact Internet Service Providers if they came across suspect material.

The group wrote on its Web site:"We feel that there will be other avenues opening to achieve our goal of a substantial reduction in child pornography and racist web sites and netizens."

The Enforcers released their statement on the Anti Online Web site, at http://www.antionline.com . The group's home page is at http://www.chronosphere.net/enforcers/ .

FTC attack online fraud

The Federal Trade Commission in the US has stopped the seller of an allegedly bogus business opportunity from making false promises on the Internet.

According to the court complaint, the FTC charged that the spam messages and Web homepage of Internet Business Broadcasting, Inc. contained "false and misleading income claims."

"Unsolicited commercial e-mail, spam in Internet lingo, is an irritant to consumers," Jodie Bernstein, director of the FTC's Bureau of Consumer Protection, said. "When the spam makes false and misleading claims, it's more than irritating, it's against the law.

"The rules for advertising by e-mail are the same as the rules for advertising through the regular mail," Bernstein said. "Don't mislead or lie to consumers, or the FTC will come after you."

The complaint, filed in the US District Court of the District of Maryland, Northern Division, is asking for a permanent injunction and "other equitable relief" against Internet Business Broadcasting Inc., Thomas Maher, Dorian Reed, and Audrey Reed.

According to the complaint, Internet Business Broadcasting and its principals claimed they operated "City Edition" Internet newspapers and sold opportunities to lease billboard or banner classified or advertising space that would run on the Internet newspaper sites.

"In spam sent to would-be investors, the defendants claimed that investors in the billboards could sublease advertising space and earn a guaranteed return on their investment," the complaint alleges. The spam messages touted the billboards as the "business opportunity (that) offers a solid return potential of 100.8 per cent the first year with only a 25 per cent occupancy rate," and guaranteed that 25 per cent occupancy rate, according to the FTC complaint.

The defendants also claimed that purchasers can "reasonably expect" to achieve earnings between $240 and $800 per month; and that the defendants "will provide a full refund of purchasers' investment if the defendants do not achieve the guaranteed 25 per cent occupancy rate, the complaint said.

The spam messages directed prospective franchisees to the defendants' Internet home page and both the spam and Internet web site offered a "guaranteed" return on investment, or a full refund to investors.

Arrest after Net sting

A chemical engineer from Oklahoma in the US who travelled to South Texas to seduce what he thought was young girl he met on the Internet now faces federal charges.

Federal agents arrested James C. Lacey after he allegedly tried to meet a 13-year-old girl he met on the Internet who turned out to be a federal agent. He is also accused of e-mailing the "girl" pornographic photographs of a young child engaging in sex with an adult.

The 51-year-old is accused of sending child pornography across state lines using a computer and for crossing state lines with the intent of engaging in sex with a minor.

The bait was put out last November by Sgt. Mickey Leadingham of the Corpus Christi police's special services division when he logged onto America Online posing as a young girl named "Ryan."

Leadingham said he notified U.S. Customs Service investigators after Lacey allegedly responded and sent photos of a girl between 8 and 10 years old having sex with an adult.

Bid to stamp out online racism

The UK Government was urged in the House of Commons to use Britain's European Union presidency to help stamp out use of the Internet to spread racist propaganda.

Labour MP Andrew Dismore said that more than 600 anti-Semitic Web sites had been set up on the Internet, many of which promoted "Holocaust denial". He urged junior Home Office minister Mike O'Brien to use the opportunity of the EU presidency to raise this problem with Europe to try to come up with a solution.

Mr O'Brien replied: "We are already doing that. We certainly condemn that sort of material on the Internet.

"The National Criminal Intelligence Service has been in close liaison with other countries to combat Internet abuse and the G7 action plan on high-tech crime commits us to developing closer links to combat Internet crime even more effectively."

Tory Dr Julian Lewis told the House: "It's possible to defame people in the foulest terms and for them to have no remedy if the Internet service provider is situated abroad."

Mr O'Brien said: "You are quite right - this is an increasing problem. We are now increasingly realising the impact the Internet can have, not only on all our lives but the types of crime."

- According to a new report, hate groups are using the Internet to spread their messages of advocating racial violence, religious persecution and other crimes.

The number of hate groups in the US rose by 20 per cent last year, according to a report by the Southern Poverty Law Centre. The group identified 163 sites on the Web used by US hate organisations, including 29 for the Ku Klux Klan, 39 posting neo-Nazi doctrine, 27 containing Skinhead messages, 25 espousing Christian Identity doctrine and 46 from various other hate groups.

Rabbi Abraham Cooper of the Simon Wiesenthal Centre, a human rights watchdog group in Los Angeles, said: "What should be of growing concern here is that we have for the first time in American history the chance to create the most powerful communications medium ever invented, and the lunatic fringe has embraced this medium."

E-mail evidence barred

Defence lawyers have been prevented from using what they say is key e-mail evidence during the trial of a student who allegedly abused a woman he had met on the Internet.

Prosecutors say Oliver Jovanovic, 31, a student at Columbia University in the Us, invited woman he had met in an online chat room to his home after a dinner date, tied her up, dripped hot candle wax on her and sexually abused her.

Defence lawyer Jack Litman said that the woman had consented, and friends of the accused said that the alleged victim had sent e-mails suggesting that she was keen on being treated roughly.

State Supreme Court Justice William Wetzel said the state's rape shield law meant that the prosecution was allowed to delete portions of the woman's e-mail messages and he said the defence could not explore her sexual history.

Wetzel also ruled that prosecutors could not back out of an agreement to refrain from using Jovanovic's e-mail against him. Assistant District Attorney Gail Heatherly had said she wanted to use his e-mail because it contradicts the defence's modified, potentially "perjurious" position.

Heatherly agreed not to use the e-mail after Litman challenged the legality of its seizure. Litman had said that any violence was consensual, but after learning there was no medical evidence of violence, he said none occurred.

In his decision, Wetzel called Litman's position "patently disingenuous and contradicted by the court record," but he said the defence has "an absolute right" to change positions as often as it wants.

Jovanovic, who graduated from Hunter College High School and the University of Chicago, is a doctoral candidate in molecular biology at Columbia. He is charged with kidnapping, sodomy, sex abuse and assault. The trial is expected to last three weeks.

Singapore Internet controls

Internet service providers in Singapore will be required by law to offer parents a way of preventing online pornography.

Information and the Arts Minister George Yeo told the country's parliament that the Internet service providers would install a filter in their servers to block access to undesirable sites.

"All Internet service providers will be required by regulation to provide parents with the option," he said. Cyber Patrol and Nanny Net were cited as examples of such filtering programmes.

He added that children were computer literate and many could gain access even to blocked sites.

Singapore has strict laws against pornography and censors films, books and the Internet and the country's Broadcasting Authority has banned some 100 Web sites that promote pornography, violence and racial or religious hatred.

"Smurf" attack caused go slow

A computer attack at the University of Minnesota in the US caused data loss and deterioration of connections throughout the entire state.

The attack lasted more than an hour, according to the university, though some targets reported feeling the effects earlier and for a longer duration.

Aimed at the university, the attack set off a chain reaction throughout the state, shutting down some computers entirely and in other cases causing data loss and network slowdowns.

It "created a cyber-traffic jam," UMN security incident response coordinator Susan Levy-Haskell said in a statement. "Users had difficulty accessing their servers and/or felt slowness in the system.

"A small number of people were totally shut down. It was necessary to down the connection to the University of Minnesota's Crookston campus, which was the target of the attack."

Hackers using the "smurf" technique flood the targeted network with replies to bogus "ping" packets, which are sent to get a response from networked computers.

In such an attack, the attacker specifies the targeted computer as the ping packet's return address and sends out enough requests to guarantee a deluge of responses.

Settlement in Net defamation

A computer user group in Australia has settled out of court in a defamation claim brought by a UK-based litigant.

Melbourne PC User Group, which acts as an Internet service provider to about 4400 members, says the case could set a dangerous precedent.

The action involved a defamation suit arising from comments allegedly made by one of its subscribers in a Usenet newsgroup in October and November 1996.

Melb PC President Stan Johnstone said in a statement: "We were dragged into this action because UK law fails to clearly recognise that an ISP carries a vast amount of Internet traffic and cannot reasonably be expected to act as a moderator between Internet users.

"This case had the potential of becoming a landmark case for ISPs and

Usenet participants alike, particularly in the United Kingdom and Australia. Although we were confident of winning, we are primarily a volunteer organisation and did not like to speculate our members' money to fight an action in the UK courts."

High tech identity theft ring smashed

The San Francisco Police Department's Fraud Division in the US says it has uncovered and arrested suspects in a high-tech counterfeiting ring.

A police department spokesperson said that Federal Postal Inspectors are also investigating and may bring charges against the seven-member group.

He said the Federal authorities were involved because of the large amounts stolen and because the group stole mail from outgoing drop boxes and from home mail receptacles,

The group allegedly used computers to reproduce fake drivers licenses, credit cards and cheques, billing victims about $5 million over the past two years, the department said.

SFPD spokesperson Inspector Earl Wismer said: "The two men in custody are the major suspects in the ring. We think they controlled the group and did the actual counterfeiting of identification cards and cheques."

Six men are in custody and a warrant is pending on a seventh "major player" in the ring, said Wismer.

The two men in custody are San Francisco residents John Santner, 32, and Eric Shay, 29. These men have been charged with more than a dozen felonies, on both state and federal charges.

Wismer could not confirm reports of $90 million in estimated nationwide losses to this kind of theft, but said this particular group had an "extensive network in Northern California with a few forays into other states, particularly Washington."

He said the group has engineered losses from two major California banks of about $4 million.

"That's just the two major banks," he said, and added, "we don't have evidence on smaller banks."

Wismer said the SFPD didn't push for federal racketeering charges because previous arrests of the group were considered too minor.

If charged individually, he said, the group would get more jail time for their crimes.

"When people try to buy a house or car," he added, "they might find that they already own a house or car, but they didn't know a thing about it. This is the crime of the `90s' — identity theft is epidemic right now."

Mitnick seeks defence witness for court

A lawyer for notorious computer hacker Kevin Mitnick is seeking an expert witness who could testify for the man, who has become a cult hero in many hacking circles.

The press release turned advertisement promises high visibility and guaranteed fees paid by the federal government. No details of the case were provided, but Mitnick's appointed defence counsel, Donald C. Randolph, Esq. seeks a multi-talented individual with expert skills in "computer security, telecommunications, system and network administration to testify in this highly publicised computer "hacking" case."

"Qualified candidates must have an advanced degree and be knowledgeable in DOS, Windows, SunOS, VAX/VMS, and Internet operations," continued the Mitnick press release.

"Experience with cellular telephone networks is a plus. Previous expert testimony and/or publication are preferred."

Mitnick is being held in prison, pending a trial this year for 25 counts related to alleged hacking activities.

His first prison term followed an intrusion into Digital Equipment Corp's computer systems. He was accused of electronically stealing $1 million in secure software from Digital Equipment Corp., causing the company to spend $160,000 to close up the gaps in its computer security.

Upon conviction in that case Mitnick was placed on supervisory probation in 1992. He disappeared later that year after he was charged with illegally cracking into Pacific Bell's computers.

Between 1993 and 1995, Mitnick evaded authorities and allegedly stole millions of dollars worth of corporate secrets, scrambled telephone networks, and even broke into the nation's national defence warning system.

He made the FBI's Most Wanted List before he was caught after breaking into the home computer systems of Tsutomu Shimomutra, a leading computer security expert at the San Diego Supercomputer Centre.

Shimomutra was so enraged that he helped the FBI track Mitnick to an apartment complex in Raleigh, using a cell phone direction finder connected to a laptop computer.

Boost for FBI

The FBI in the US plans to spend $430 million over the next five years to modernise its global information gathering and analysis systems.

The FBI said the Information Sharing Initiative, which will be spread across three phases, will be a boost for investigators and greatly improve operations.

"This is an important contract because it is critical to accomplishing FBI operations, providing access to the information as needed and increasing efficiency," said Mark A. Tanner, special assistant to the FBI's deputy director.

Through ISI, the FBI plans to develop an integrated system to support criminal investigations and counter-intelligence initiatives.

The bureau wants to buy an estimated 15,000 PCs, 5,000 scanners, 3,000 printers and hundreds of servers.

During the initial phase, the FBI also wants to deploy multimedia and document management systems that will let users electronically capture all investigative and counterintelligence data, including text, image, video and audio files.

In phase two, the FBI will deploy analytical and intelligence tools along with database applications and in the final phase security network applications and gateways, along with encryption equipment and e-mail and Internet servers will be installed.

Product news

Web site search tool checks copyright

A company specialising in trademark and copyright services has announced a new version of its search tool for checking the Internet.

US firm Thomson & Thomson, has released a print report version of its new SiteComber Search product.

The company claims the system is the first and only tool designed specifically for searching Web pages for common law occurrences of trademarks on the Net. These trademarks are not registered, yet still possess legal rights because of their use in the marketplace.

T&T now offers SiteComber Search as a print report and this enables clients to order over the phone from the firm's client services group and receive a printed report delivered via FedEx.

Jay Gast, president of Thomson & Thomson, said: "SiteComber Search 'combs' Web sites, locating pages that contain identical character-string matches of proposed trademarks."

"The introduction of the print product means clients can easily request a SiteComber Search at the same time they order other trademark research.

SiteComber Search pairs the proposed trademark with up to three international classifications and additional keywords, and provides an easy-to-read list of citations, ranked and in context.

For more information contact Donna Summerville, corporate marketing manager of Thompson & Thompson on (US) 800-692-8833 or +1 617-376-7665, donna—summerville@thomson-thomson.com/ or visit the firm's web site at www.thomson-thomson.com/

Web theft insurance

Software that embeds a 'digital fingerprint' into pictures and images to provide evidence of ownership has been combined with an insurance policy to counter wholesale piracy.

Thousands of images are stolen every year from picture libraries, newspapers, magazines and photographers and up until now copyright holders have had little or no redress. The package has been launched by New Mexico Software, which has developed a form of digital fingerprinting called SureSign.

"When combined with the insurance policy, the new protection system, NMS CoPs, will deter pirates who infringe the copyright on more than 30 per cent of all pictures," said Norman Milne, UK Managing Director of New Mexico Software.

He added: "Publishers, picture libraries, image agencies, photographers, illustrators and artists can now display photographs on the Internet and CD's with the knowledge that their images are protected on a worldwide basis."

The insurance policy, referred to as picture insurance, is underwritten by Beazley at Lloyds of London and was developed by CE Heath.

David Nicholson, who underwrites the policy at Beazley, said: "This represents the first of a suite of products designed to work in conjunction with specific new technologies in encouraging commerce on the Internet.

"The policy when combined with NMS CoPs will help give owners and sellers of images the comfort they need to use the full potential of digital picture technology and the Internet."

Until now, many pirates, often large organisations, felt safe in the knowledge that a photographer or a picture library would not be able to afford to pursue copyright law infringements due to the high cost of litigation.

Alan Bartlett, Marketing manager for Signum Technologies, who developed the software said: "As the demand for images grows, content providers must protect their valuable material with the most effective means possible."

Annual premiums will start at £110 and premiums include an annual license for the use of SureSign fingerprinting software.

Contact Roland Miller, New Mexico Software Ltd, tel: +44 (0) 411 759460, fax: +44 (0) 1992 509767, e-mail: rolandsiteguard.net or visit the web site at WWW: http://www.image-assets.co.uk

In the US contact New Mexico Software Inc, on +1 505 856 4075 or visit the web site: http://www.image-assets.com

Cyber monitoring

US firm Pearl Software has announced the latest version of its Cyber Snoop program for tracing a computer user's Net activity.

The system is aimed at parents to help supervise Internet use and to protect themselves and children from common dangers and abuses, but can also be used to follow anyone's Web movements.

Its makers claim Cyber Snoop V 3.0 can retrace every step an Internet user makes by creating a complete audit trail of Internet activity, including Web Sites, FTP, News, Chat, and e-mail.

The Quick Link feature allows the administrator to automatically link back to the Web sites that have been visited. It also restores the text of incoming and outgoing News, e-mail and Chat items, allowing the administrator to catch predators who attempt to abuse minors.

Version 3.0 features Web-Chat tracking, and a keyword blocking option which helps safeguard against dissemination of personal information. This newest version of Cyber Snoop also captures the Windows user name for display in the Cyber Snoop Log, allowing the monitoring of machines with multiple users and eliminating the need for sign-in sheets. If perpetrators are identified, Cyber Snoop V 3.0 provides automatic links to appropriate law enforcement resources.

The software operates on a Windows 95 or NT platform and costs $39.95. For more information contact Pearl Software on +1 610 458 2387 or visit the Web site at www.pearlsw.com.

Real time recognition puts people in picture

US firm Visionics say its FaceIt DB system can match a known suspect's face instantly with an image taken from a live camera.

Applications could include an airport, where a computer linked to a surveillance camera matches a passenger's face to a terrorist's, or a convicted shoplifter could be electronically spotted within minutes of the suspect arriving in a store. And the company also says

the program can analyse Internet images of exploited children, and a comparison of each child's face against a database of missing children can instantly identify some of the subjects.

FaceIt DB can search live video of large crowds in real time for faces on a watch list and alert administrators to any matches, eliminating the need for security personnel to continuously monitor video screens. In addition, the program can build a time-stamped database of all faces that pass by a surveillance camera for later analysis.

"Sophisticated algorithms that can replicate the way the human brain recognises faces have opened up a whole new area of opportunity for law enforcement and security, with applications ranging from welfare fraud to federal investigations," said Dr. Joseph J. Atick, Visionics CEO.

FaceIt DB runs on Microsoft Windows 95 or Windows NT. The internal database representation of each face is fixed, regardless of the image resolution, at a size small enough to allow 1 million images to reside on a standard multiple gigabyte hard drive. The system can accept digital images in standard file formats including JPEG and TIFF.

For more information, contact Visionics at +1 201-332-9213, fax +1 201-332-9313 or visit the Web site at http://www.faceit.com.

Security audit

Companies are at risk from an ever-growing number of hackers, corporate spies and fraudsters all trying to break into their systems.

To help corporations combat the security threats posed by the Internet, Metamor, a Chicago-based software development and IT consulting firm, has launched a new security audit service incorporating the latest security technologies and tailored to the business needs of companies.

The Metamor Internet Security Audit is a comprehensive review of a corporation's computer systems and networks and includes security policy development, network security analysis, network security testing and encryption and data protection strategies.

"A security breach jeopardises a company's critical business data, its resources and its reputation," said Brian Farrar, principal at Metamor's Internet and Intranet services group.

"Many companies are unaware of the design flaws and security holes in their networks and servers, either because they have never been attacked, or they have been attacked but didn't detect the intrusion. What's more, the financial loss from a security breach can be significant."

The Internet and Intranet Services group at Metamor specialises in commercial Web development, Intranet applications, electronic commerce, security, and document management and imaging systems.

For additional information contact Metamor, tel: +1 312 251-2000, Fax: +1 312 251-2999 or visit the Web site at www.metamor.com

Laser fingerprints

Laser technology is being used to get fingerprints from crime scenes where normal techniques fail.

The system, developed by Spectra-Physics, obtains fingerprints that are normally considered unrecoverable using traditional methods.

In these cases, laser-enhanced fingerprints provided the principal evidence linking the guilty party to the crime scene and directly contributed to the resulting conviction.

Recent cases include recovering fingerprints from a crumpled silver chewing gum wrapper, from tiny pieces of a smashed cash register and from a plastic bag which had contained drugs. In all cases the prints resulted in convictions where the suspect might otherwise have walked free.

"A fingerprint identification by a qualified examiner is 100-percent conclusive. Forensic fingerprint evidence is by far one of the most damaging pieces of evidence there is for a criminal," said Michael Murphy, supervisor of the Latent Print Section at the California Department of Justice.

Lasers typically are used to improve the contrast of the image on surfaces that are textured or not normally conducive to normal fingerprint powders. The print is developed using a superglue, then rinsed with a dye, which adheres to the superglue-developed print.

The laser's high-power, 532-nanometer (nm) green beam excites the dye, causing it to fluoresce and produce an image that an examiner can photograph with a 35-mm camera or with new digital technology.

For more information contact Spectra-Physics on +1 650 966-555 or visit the firm's web page at http://www.splasers.com

Firm given go ahead for encryption

A US firm supplying encryption technology has announced plans to sell its sophisticated scrambling products overseas, bypassing strict export controls.

Network Associates Inc. said it would sell its Pretty Good Privacy (PGP) encryption software in other countries through a deal with a Swiss company, cnlab Software.

The software scrambles e-mails and files, preventing eavesdroppers from seeing information sent across the Internet and stored in databases.

Network Associates said work on the PGP encryption products would be done in Europe using code legally exported from the US.

But the move could spark a reaction from the US Commerce Department, which controls encryption export in an attempt to stop criminals using the programs to hide sensitive information.

Undersecretary of Commerce William Reinsch said: "We're going to have to look at it very closely to see if it violated U.S. law or regulation."

The government will seek to learn whether the company illegally exported any encryption to make the products abroad and will also directly review the products, which could be subject to US export rules if they contain more than 25 per cent domestic content.

Reinsch said the government was "disappointed" about the Network Associates deal. "It's not consistent with our

policy and we're always disappointed when people do things that make our job more difficult," he said.

He added: "If you've got international terrorists and international drug dealers engaged in crimes that transcend national borders, you need ... communications that are recoverable."

Network scanning

Software to probe networks in an attempt to identify vulnerabilities to hacker attacks has been launched by US firm Axent Technologies.

NetRecon looks at the risks both from the Internet and from internal users and it automates the process to minimise disruption. The company says the system can scan multiple devices (for example routers, mainframe, and firewalls), run multiple protocols on multiple operating systems and minimise the network load the scan produces on a network.

"NetRecon gives us that outside expert's perspective of how secure your network is," Rob Clyde, Axent's vice president of security management, said.

"We see it fitting in nicely with Enterprise Security, which gives you the inside view on how you do against certain practices and you also can use it to test intrusion detection software."

NetRecon, available now through the company or its resellers, is priced at $1,995 for limited use or $9,995 for a license to scan an unlimited number of networks. For more details contact the firm on the Web at http://www.axent.com/

Password cracker

A new password cracking program has been launched by a group that last year hit the headlines with its code for getting into Microsoft Windows-based software.

Lopht Heavy Industries said the latest version of its "lOphtcrack" code is a tool for systems administrators and security professionals concerned about potential points of access in their local networks.

New functions now allow passwords to be intercepted across a local network from NT or 95 machines that use the older LAN Manager authentication system. With updated NT authentication, passwords cannot be intercepted.

A previous version of lOphtcrack allowed a hacker to retrieve "hashed" or encrypted passwords from an NT machine after administrative access had been gained. Those passwords could then be victims of a "dictionary attack" in which a software program runs through potential passwords until it guesses them correctly.

The latest version also allows the user to pick off passwords as they are being sent across the network to the machine to which the user wishes to gain access.

Information on the group's Web site promises: "It's big. It's bad. It cuts through NT passwords like a diamond-tipped steel blade. It ferrets them out from the registry, from repair disks, and by sniffing the Net like an anteater on dexadrene."

The lOphtcrack tool is available for free on the company's Web site but includes a time-out mechanism that renders the software useless after 15 days. In order to keep the latest version, users must pay a $50 fee.

Spammers back with backbone

The self-proclaimed kings of spam are back, but they say they will now adopt a fairer and gentler approach to junk e-mail.

Global Technology Marketing Incorporated, a joint venture between spam companies Quantum and Cyber Promotions along with an unnamed access provider, will offer customers set marketing price plans.

Walt Rines, notorious spammer and president of GTMI and his colleague, fellow spammer and chief executive of the firm Sanford Wallace, vow to "put e-mail marketing on the same playing field as junk [snail] mail, telemarketing, and other forms of marketing that are accepted."

GTMI's site was advertising the company's "unique vision for the future of Internet marketing and promotion." Monthly pricing for connectivity runs the gamut from T1 access for one year at $5,900 per month up to T3 access for 60 months for $73,500 per month.

The problem of spam mail has escalated to such a degree that lawmakers on state and federal levels have introduced bills trying to curb the problem.

Aside from the uproar in the Net community about the overall problems with the volume and nature of bulk e-mail, access providers have complained as well. Internet service companies say they end up paying to process the spam, which at times clogs their servers. Some have brought lawsuits against spammers, many of which have been successful.

GTMI says the answer to this problem is to compensate the providers for their inconvenience, or looked at another way, pay them to carry spam.

Many ISPs however will be worried about the reaction of their customers who object to junk e-mail. Rines said this shouldn't be a problem, as the ads would mean a lower cost of access.

"At least it makes things the way they should be," Rines said. "Then it is up to the provider to pass the revenue stream on to the customers."

Another complaint Net users have about junk e-mail is the unseemly nature of the ads, which sometimes advertise pornography and get-rich-quick scams.

Rines said those practices will not be accepted by GTMI: "The quality of ads needs to improve." Also, GTMI will not accept "porn, fraud, or anything illegal or obscene," he added. He said that the company, in its quest to legitimise spam, would not allow its clients to avoid blocks or break the law in any way.

Rines added: "People hate ads - I hate them. But [users] know they're getting a benefit. They know they don't pay $20 for an issue of Newsweek because advertisers are subsidising those costs.

We think the market will tell whether people want to pay more for access on an e-mail-marketing-free network," Rines said.

He recognised that his reputation, along with those of Wallace and other spammers, would be a hurdle.

"Ironically, Sanford and I are the most qualified to do this type of business, but we're the least likely to be given a chance," he said.

Court reports

Judge condemns filth on the Net

A judge said that the Internet contained "unwholesome and unnecessary filth" as he gave a student a suspended prison sentence for pornography offences.

In what is thought to be the first case of its kind, 21-year-old Timothy Spring pleaded guilty at Preston Crown Court in the UK to four charges of publishing obscene articles on the Internet.

The media studies student was prosecuted despite setting up his web site in the US in a bid to evade UK law.

Superintendent Martin Jaunch of Scotland Yard's vice unit said after Spring was given an eight-month suspended sentence: "This has proved that the Internet is not a sort of Wild West where the law does not apply."

Spring, a University of Central Lancashire student, of Kirkham, near Preston, also pleaded guilty to six offences of having 5,000 indecent photographs of children which the court was told he had downloaded from the Web.

Working from his bedroom in his parents' home, he placed hard-core pornographic images of adult sex on his US web site, which had recorded more than 100,000 'visits' by computer users.

Sentencing him Judge Reginald Lockett said: "It seems to me that readily available on the Internet in and around this world is a lot of unwholesome and unnecessary filth. I am told that it is available if you know which buttons to press."

Spring had set up a web site through a UK provider which gave users access to the US site carrying the pornography.

Supt Jaunch said the case proved that police could successfully prosecute Internet pornographers even though material was stored on a Web site set up in a foreign country.

He said: "We have proved the current legislation is flexible enough to allow us to take action and apply the existing laws even though they might be 40 years old."

John Wilson, defending, said Spring "entered a world where he could attract people's attention. Hundreds of thousands of people visited his site and it was the buzz of this which excited him."

Spring's sentence was suspended for two years and he was also given a 12-month supervision order.

Tax worker's fraud

A former Internal Revenue Service employee in the US has admitted accessing IRS computers to unlawfully prepare tax returns.

According to US Attorney Faith S. Hochberg, Ertha McCoy, 40, of Montclair, New Jersey, pleaded guilty before US District Judge Joseph E. Irenas to a one-count felony charging her with exceeding her authority in accessing IRS computers and obtaining information for private financial gain.

When McCoy is sentenced on June 12 by Irenas, McCoy will face a maximum of five years in federal prison and a $250,000 fine. In her plea, McCoy said she was a tax assistant, authorised to use the IRS's computerised Integrated Data Retrieval System to access taxpayers' confidential files and accounts.

According to court records, McCoy acknowledged that those rules and regulations prohibited IRS employees from preparing income tax returns for compensation but admitted that she prepared, and sometimes was paid to do this for friends and relatives.

Man "hijacked" Web in net naming case

A man who tried to set up an alternative to the Internet naming service admitted computer fraud after he stopped thousands of Net users from reaching his competitor.

AlterNIC founder Eugene Kashpureff, 33, of Belfair, Washington, pleaded guilty in a Brooklyn federal court to one count of computer fraud. Kashpureff faces a possible maximum sentence of five years in prison and a $250,000 fine.

The charges against him alleged he designed and implemented a software system, which blocked Internet users worldwide from reaching the Web site for the InterNIC, which administers Internet addresses.

His system supposedly "hijacked" users to his "AlterNIC" site on the World Wide Web. The software was effective through July 10 and July 14, 1997, and from July 21 to July 24, 1997.

Kashpureff was arrested and extradited from Canada where he had lived since learning US authorities had a warrant for him. And he boasted he could divert all communications destined for China, the 100 most-visited Web sites in the world and the White House Web site. According to reports, he called his scheme "Operation DNS Storm."

InterNIC, which is owned by Network Solutions Inc, administers more than 1.2 million domain names, and its Web Site is visited over the Internet about one million times per day.

Sentence for porn

A computer engineer was jailed for 78 months for receiving an explicit picture of a girl that he had met over the Internet.

Richard C. Crandon, a 39-year-old computer network engineer from New Jersey received the picture of a 14-year old from a photo finisher in Seattle.

Crandon, of Long Branch, New Jersey, pleaded guilty last November to a one-count federal indictment charging that he received the photographs in late summer 1997 of the girl engaged in sexually explicit conduct.

Crandon's crime began with an Internet conversation with the young victim, a Minnesota resident, and he travelled to Minnesota at least twice to see the young girl and took her photograph.

US District Judge Harold A. Ackerman sentenced Crandon to 78 months in federal prison, ordered him to pay $57,050 for psychiatric care for the girl and to serve a three-year probation term after imprisonment.

US Attorney Faith S. Hochberg said: "Too many children are being victimised by predators and paedophiles who hunt their young prey over the Internet.

"Receiving sexually explicit photographs of minors whether by mail or by a computer is a serious federal crime."

"Before our children go on the Internet, we need to warn them about the dangers lurking there."

Internet Watch Foundation

After a year of operations, the Internet Watch Foundation says it has helped rid the Internet of more than 2,000 undesirable Web pages.

The IWF is an international group of Internet industry, independent and non-profit organisations concerned about promoting free speech on the Internet in a regulated way to stop children getting access to unsuitable material.

In the first annual report, the IWF says that it received 781 complaints referring to 4,300 items on the Net in the 12 months since it established a complaints hotline.

Barbara Roche, the UK's Department of Trade and Industry Minister, welcomed the work done by the IWF, but also announced a government review of its role aimed at widening the work it does. She said: "The partnership approach between Government and service providers is making an impact. It's not a soft option, but backed by the full force of the law.

"However, we are not complacent and recognise the need for further progress to be made. Our review of IWF will help identify where action is needed and set the future priorities for the organisation.

The Internet offers unrivalled opportunities to individuals and business and we must ensure they are not compromised by an unprincipled minority.

"The Government is not complacent about illegal and harmful material on the Internet and we intend to uphold the law online as we do off-line," she said, adding that the government is keen for the IWF to maintain the momentum.

Roche's comments come when strong rumours are circulating that the government and police are looking seriously at prosecuting Internet service providers in the UK for allowing access to the so called illegal Usenet groups.

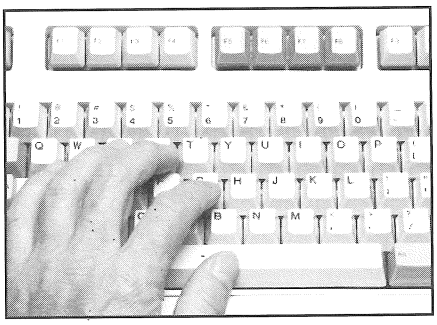
These Usenet groups, thought to number about 50, and which have been barred by many ISPs in the UK and the US, can act as message exchanges for paedophiles.

Several ISPs, notably Demon Internet Services in the UK, do not bar access to these newsgroups, on the grounds that this merely sends the problem image files spinning into other, more legitimate, Usenet newsgroups.

According to the IWF, meanwhile, its annual report shows that up to 95 per cent of the 2,000 items removed as a result of IWF action contained images of children engaged in sexual activity.

However, officials acknowledge that the foundation has only been able to catch a "very small proportion" of the total illicit material on the Internet.

The IWF report notes that, while many complaints refer to around 40 Usenet newsgroups, there are more than 27,000 groups available, making policing them a difficult task.



David Kerr, the IWF's president, said that the foundation knows it has not got all the material , "but we do have a better idea of where it is coming from."

"Service providers cannot effectively monitor the vast amount of material generated by organisations and individuals, so the Foundation is keen to publicise its hotline more widely and harness the energy of the Net-using public against abuse of the medium.

He added: "One of the biggest worries is the availability of child pornography, represented in 85 per cent of complaints. All reported material has been removed."

Kerr said that software, which can find sites likely to contain illegal material, is being developed and should be available within the next six months.

The IWF is working to develop an extension of the PICS protocol developed by the World Wide Web Consortium. At that time, Kerr said that the foundation has agreed to develop a coded means of describing Internet content, which can be used worldwide.

The idea behind the system is that a description will be contained in a label generated by the content producer using guidelines and software developed by the new International Working Group for Content Rating.

Along with the report from IWF, Kerr said the foundation's research suggests that around six per cent of illicit material originates from UK sites, with 19 per cent (and growing) from Japanese sites. A large 63 per cent, the IWF claims, comes from US sites. The IWF's Web site is at **http://www.iwf.org.uk**.

Detective Chief Superintendent Keith Akerman, chairman of the Association of Chief Police Officers' Crime Committee's Computer Crime Group and head of Hampshire CID, said: "We are concerned that public awareness of computer crime issues in general is still very low.

"Computing technology and the Internet offer legitimate benefits to business and education in particular, but they also offer the same advantages, and more, to criminals.

"We feel particularly strongly that the Internet, which is now part of the infrastructure of society is especially vulnerable to criminal attack.

"It needs protecting by a regulation or policing effort requiring international co-operation that has never been needed in the past. Police are very keen to develop a positive working relationship with the Internet Service Providers, in our mutual interest."

The IWF is also working to establish an international rating system for legal material which would allow users to avoid seeing, or allowing their children to access, anything on the Net they would personally find unsuitable.

The Department of Trade and Industry review of the IWF will report back to the Government in autumn and among the topics to be covered are compliance of the Internet Service Providers, usage of filtering and rating tools, adult pornography, racist material and breaches of copyright.

The NCH Action for Children group in the UK has welcomed the work of the IWF and has also published a booklet on the opportunities and hazards of the Internet to help parents. "Internet - Opportunities and Hazards" available from NCH Information, telephone 0171 704 7121.

Inadmissible evidence?

It is generally accepted that for all practical purposes, information stored on magnetic fixed disks can be altered without trace.

This does not mean that there will be no trace, simply that when new data is written it reduces the pattern of the original data that it replaces, to such minuscule traces as to be practically indecipherable.

It is this property above all others which makes the forensic investigation of computer contents so necessary. There are a number of different commercial devices which provide varying degrees of integrity protection when copying data from computers for forensic purposes.

Arguments continue over which is best, which is the most efficient, which is the cheapest, which the most secure. As far as evidential integrity is concerned, such arguments are largely irrelevant.

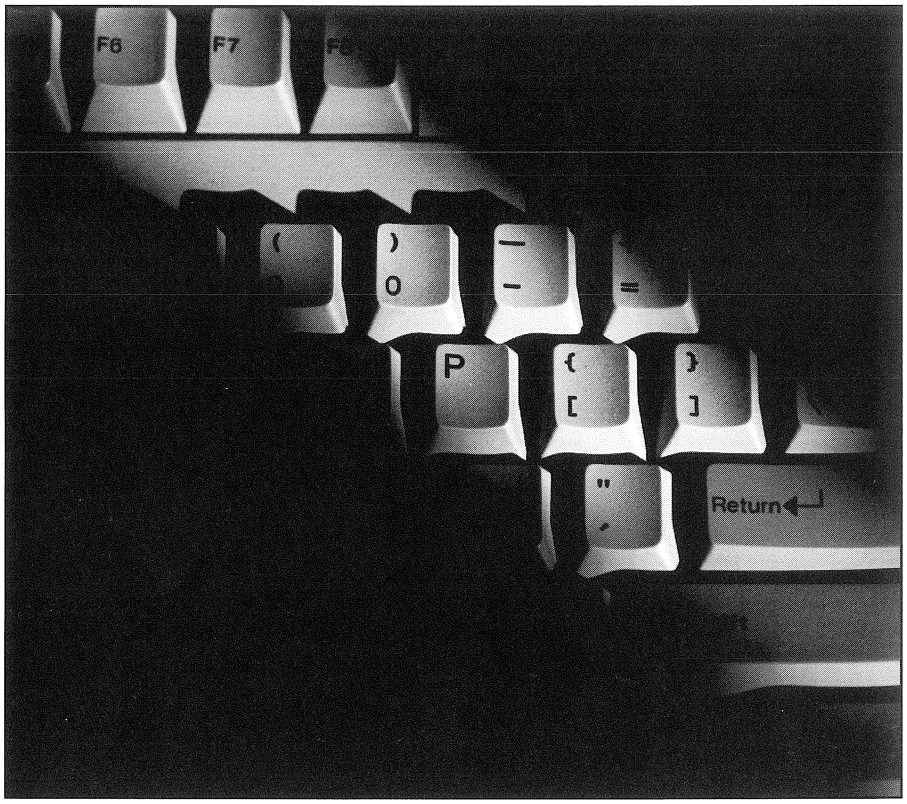
The security (or otherwise) of a copying method can only be verified by the designers and manufacturers of the process. Their company must stand or fall upon the accuracy and reliability of their product and it is certain that a single rejection on either of these grounds would be sufficient to destroy the product permanently.

Thus the investigator is freed from responsibility for the copying mechanism - he simply calls in the supporting company and lets them support their own procedures.

Inadmissibility

What is much more relevant are the procedures used to collect and investigate the material in the search for evidence. The courts rightly insist upon stringent standards of evidential security and continuity but the final integrity of computer evidence relies heavily upon the honesty of the primary investigator.

For example: regardless of the copying device being used, the simplest way to plant evidence would be to do so before the copying took place. At the lowest level technically, any modifications introduced in this way would be on all copies (even sealed security copies) and impossible to detect in isolation. However, experienced forensic practitioners will immediately realise that modifying material in a meaningful way and without introducing unresolvable inconsistencies is either extremely difficult or very time consuming.



It has been suggested that if there is any indication that the contents of a machine have been modified whilst in the hands of the investigators then the whole lot should be declared inadmissible. This apparently solves the problem in most cases but what if the suspect deliberately introduces what appears to be planted evidence before the machine is examined and thereafter argues that all of the material is thereby compromised?

This is not a likely scenario at the moment but a growing awareness of the nature of computer material might well make it more likely in the future.

A case history

There are other aspects of this problem, some of which were highlighted during a recent investigation into the alleged possession of images of child pornography.

While the details had no bearing on the final outcome of the case (the defendant pleaded guilty), the questions raised were so fundamental that they are presented here for general information and discussion.

The chronological sequence of the forensic examination has been altered in this description to emphasise the importance of the observations and conclusions.

The investigation was undertaken for the defence and the seized material included a Personal Computer with a 2 Gb hard drive, a ZIP drive and five ZIP disks. The PC hard disk had been recently defragmented but contained some pornographic images and evidence that they had been downloaded from web sites and usenet groups on the Internet.

Four of the ZIP disks appeared to be unused but the fifth one contained a quantity of pornographic images - some of which involved children. Most of the evidence presented by the Police was taken from this ZIP disk.

The defendant in his original statement claimed that all of the evidential material had arrived on his machine as a result of him subscribing to certain newsgroups.

He had copied it to the ZIP disk without viewing it and had intended to view it later - deleting any unsuitable material

as he did so. Had he been aware of the illegal nature of some of the material he would have deleted it immediately. The defendant had been charged under Sections 160(1) and (3) of the Criminal Justice Act 1988. Section 160(2) (b) of this Act allows a defence if the material has not been seen and is not known to be or suspected as being indecent.

This is a common defence in the UK to charges of this sort where computer material is involved because subscription to a newsgroup means that messages are sent automatically when the user connects to his ISP.

Such messages are transferred unseen and may contain graphic images, the content of which is not apparent until the user elects to view them.

The PC hard disk was configured for use by Windows 95 and contained some 1.1Gb of active data. Evidence of heavy Internet use was found, together with details of newsgroup subscriptions and direct access to a number of Web sites (using Internet Explorer 4).

There were some pornographic image files and evidence that some of these had been downloaded via browsing (rather than via newsgroup e-mail). Defragmentation meant that an active structure analysis revealed little of any consequence.

However, traces of files and directory entries were found in slack and unallocated areas which indicated the presence, location and some content of previous directory structures.

The ZIP disk contained a total of fifty-four directories, all of them containing quantities of pornographic image files but only nine of them contained images that involved children.

The names of the directories and their contents indicated that the files had been sorted into related groups. In most cases these related groups all had similar filenames (BLOND01.JPG, BLOND02.JPG, BLOND03.JPPG etc.) but two of them had a wide range of filenames and the indications were fairly conclusive that the files had been sorted according to their graphic content.

There were even some instances of similar filenames in different directories (BOY01.JPG, BOY02.JPG etc.) where the content was the linking factor. All of this provided compelling indications that someone must have viewed the content in order to correctly complete the sorting.

It is never possible to prove from computer material alone that a specific person has viewed certain files. However, it may be possible to show that someone has viewed files if certain graphics software has been used.

In this case for example, the graphics package PaintShop Pro was present on the disk and the browser option had apparently been used to view files within certain directories, leaving behind a telltale browser file (written by the PSP package).

This browser file contains not only the names of the files browsed, but also a thumbnail representation of their graphic content and details of the drive and directory in which they reside.

The date/time stamp of the browser file may also be an indication of when the files were viewed. This information remains even after the original files have been deleted.

Thus in one directory named "Best of Boys Will Be Boys" for example there were 47 files named BWBB01.JPG to BWBB73.JPG - only the numbers varied within the file names and they were not in any obvious sequence.

The co-resident browser file indicated that a directory called D:\Best of Boys Will Be Boys had been browsed and that 47 files with names running from BWBB01.JPG to BWBB73.JPG in the same sequence were in the directory at that time.

This is pretty compelling evidence that the browser file had been written into that directory during the process of browsing (rather than being copied from elsewhere).

On the ZIP disk, there were a total of 30 browser files (named PSPBRWSE.JBF) - all nine of the directories that contained images of children also contained browser files.

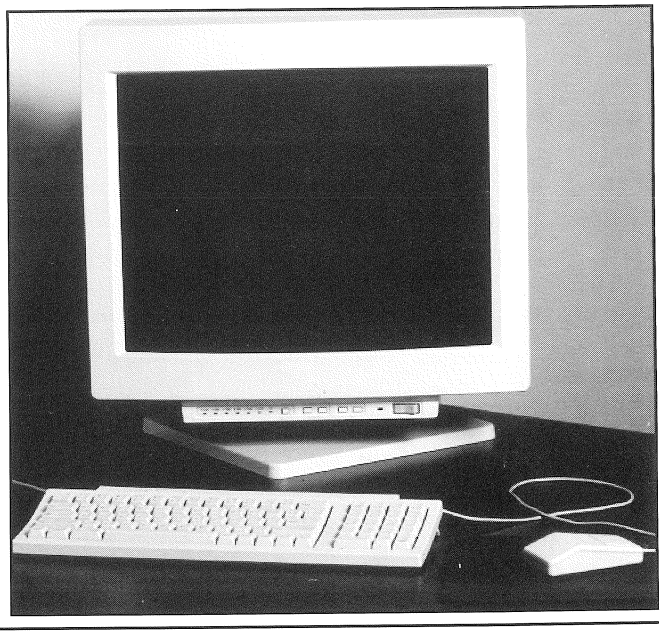
The content and in some instances even the order of the image file names matched the directory contents to a high degree and the inevitable conclusion was that the files had been viewed by somebody.

Some of the browser files indicated their original use on drive C:, others on drive D: and still others on drive F:. Analysis of the PC configuration indicated that the ZIP drive appeared as drive D: and it seemed (from the observations above) that some of the directories were therefore browsed directly on the ZIP disk itself.

The drive C: indications were probably in browser files copied along with the image files from the hard drive to the ZIP disk. It should be noted that the PSP browser file is usually only written on first access when no valid browser file is detected in the target directory.

There is also a sort option which may alter the order in which file information appears within the browser file. The drive F: indications could have arisen either by copying or by access to the ZIP disk on a differently configured PC.

Thus it is easily within the bounds of possibility that the suspect could have taken (or loaned) the ZIP disk to a friend who also had a ZIP drive and copied the files there.



Further analysis of the contents of the browser files and the fragments recovered from the PC hard drive confirmed such a high degree of similarity that it was possible to reconstruct an almost complete directory tree showing how the fixed disk would have appeared before defragmentation.

The conclusion was that it was very highly probable that a large proportion of the pornographic image files (including those of children) had been browsed on the hard disk.

Contamination

All of the foregoing is interesting but it is nothing more than a description of normal forensic analysis. What makes this case of special interest is the fact that six of the browser files on the ZIP disk (including two in the directories containing images of children) were dated after the police had seized the machine.

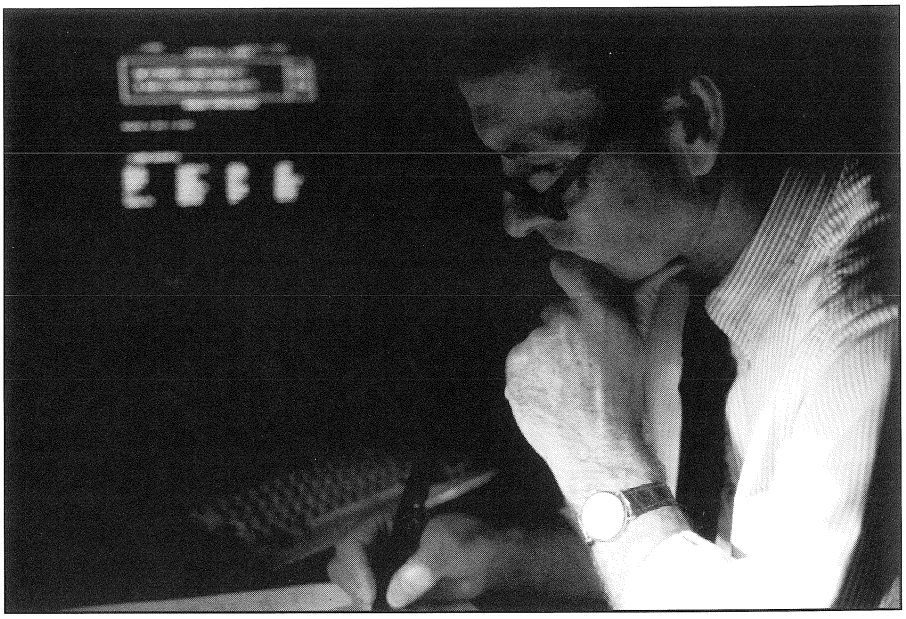
It should be noted in passing that this fact was known right at the start of the defence examination when the initial evaluation of the material was completed.

The defence forensic investigation had been conducted on image copies of all of the original material but enquiries revealed that the Police during their investigations had not copied the ZIP disk.

There is no physical write-protect mechanism on a ZIP disk and the police did not attempt to either copy the disk as an image or copy the files individually. Instead they had directly browsed certain directories on the disk, selected certain files and then copied and printed them for presentation as evidence.

They were not aware that their own browser (a different version of PaintShop Pro) would write browser files to the original disk. So, these six files constituted admitted contamination of the evidence in a case where the contents of a browser file might be crucial. Not only were invalid browser files present, but they had overwritten a significant amount of space on the ZIP disk, possibly destroying vital evidence in the process.

Further examination recovered the contents of the original browser files and tests determined that the Police PSP browser had been unable to read the original PSPBRWSE.JBF files and had



therefore deleted them and written new ones based upon the current contents of the directory.

These were in fact all the browser files containing indications of drive F: within them.

The questions

As noted above, these findings had no effect on the eventual outcome of the case because the defendant pleaded guilty when the extent of the material discovered on the hard disk became apparent.

However, the contamination of the ZIP disk revealed negligence on the part of the Police. As noted above, it has been suggested that any contamination should invalidate the remaining contents. Since this was demonstrably the result of negligence, should it be argued that not only the ZIP disk but all of the remaining computer evidence (including the hard disk) should have been declared inadmissible?

Alternatively, detailed analysis easily identified the exact extent of the contamination and it might be argued that this very same analysis confirmed the integrity of the remaining data on the basis that the contamination was negligent rather than deliberately malicious.

The question also occurs - what if it were not contamination but general corruption that occurred?

The usual assumption is that planted evidence is intended to show guilt but what if a corrupt investigator were to introduce contamination or corruption deliberately, with the intention of ensuring that all of the computer material should thereby be declared inadmissible?

It seems that there can be no clear cut answer. As with most of these apparently academic problems, the solution appears to lie in the specific practical details of each case.

Is it therefore incumbent upon the honest investigator to confirm or deny that discovered evidence is consistent with normal computer operations? What if two investigators produce different interpretations of the same material and are unable to agree which is more likely?

In the UK we are still in a honeymoon period where computer based evidence is concerned.

Correctly secured and investigated evidence is accepted with little question but as the pace of the chase increases it is our responsibility to ensure that such vital material is secured properly, investigated accurately and presented fairly.

Case study - airport hacker

A juvenile computer hacker in the US was arrested after he cut off communications at an airport control tower as well as gaining access to confidential records and disabling a town's phone system. **Paul Johnson** looks at how the hacker gained access to the computers.

In the first case of its kind in the world a minor has been arrested for using his computer to disabled a key telephone company serving a regional airport in the US.

As a result of a series of commands sent from the hacker's personal computer, vital services to the Federal Aviation Administration control tower at Worcester, Massachusetts, were disabled for six hours in March of 1997. In the course of his hacking, the defendant also broke into a pharmacy computer and copied patient records.

The charges, by United States Attorney Donald K. Stern and Acting Special Agent in Charge Michael T. Johnston of the US Secret Service, have only just been revealed and are the first ever to have been brought against a juvenile by the federal government for commission of a computer crime.

US Attorney Stern said: "Computer and telephone networks are at the heart of vital services provided by the government and private industry, and our critical infrastructure. They are not toys for the entertainment of teenagers.

"Hacking a computer or telephone network can create a tremendous risk to the public and we will prosecute juvenile hackers in appropriate cases, such as this one."

Acting Special Agent in Charge Johnston said: "This case, with the associated national security ramifications, is one of the most significant computer fraud investigations conducted by the US Secret Service."

The criminal charges allege that the computer hacker temporarily disabled Next Generation Digital Loop Carrier systems operated by NYNEX, now owned by Bell Atlantic, at the Worcester Airport and in the community of Rutland, Massachusetts.

Loop carrier systems are programmable remote computers used to integrate voice and data communications originating on a large number of standard, copper-wire telephone lines for efficient transmission over a single, sophisticated fibre-optic cable.

The loop carrier systems are used by telephone companies to integrate service provided over hundreds of telephone lines for digital transmission over a single, high capacity fibre-optic cable to a central office.

"Just as disabling a circuit breaker box blacks out an entire house, so disabling a loop carrier system cuts off all communications with the telephone lines it services," said Stern.

The loop carrier systems operated by the telephone company were accessible from a personal computer's modem so that telephone company technicians could change and repair the service quickly from remote computers.

The hacker identified the telephone numbers of the modems connected to the loop carrier systems operated by the telephone company providing service to the Worcester Airport and the community of Rutland, Massachusetts. On March 10, 1997 he accessed and disabled both in sequence.

At about 9am, the juvenile computer hacker intentionally, and without authorization, accessed the loop carrier system servicing the Worcester Airport. He then sent a series of computer commands to it that altered and impaired the integrity of data on which the system relied, thereby disabling it.

Public health and safety were threatened by the outage which resulted in the loss of telephone service, until 3.30 pm, to the Federal Aviation Administration Tower at the Worcester Airport, to the Worcester Airport Fire Department and to other related concerns such as airport security, the weather service, and various private airfreight companies.

And as a result of the hack, both the main radio transmitter, which is connected to the tower by the loop carrier system, and a circuit which enables aircraft to send an electric signal to activate the runway lights on approach were disabled for this same period of time.

Later on the same day the hacker accessed the loop carrier system servicing customers in and around Rutland, Massachusetts and he sent a series of computer commands to the digital loop carrier that altered and impaired the integrity of data on which the system relied, thereby disabling it. This disrupted telephone services throughout the area and during this attack, the juvenile computer hacker changed the system identification to "Jester".

It is also alleged that, in a separate computer intrusion, the hacker broke in to a pharmacist's computer in a Worcester area branch of a major chain.

The pharmacist's computer was accessible by modem after hours when the pharmacy was closed to allow the store to transfer information from the local computer to a centralized system.

The juvenile identified the telephone number associated with the modem servicing the pharmacist's computer in the Worcester pharmacy. On each of four occasions he instructed the Worcester pharmacy computer to transmit to his personal computer files containing all of the prescriptions filled by the pharmacy during the previous week, detailing them by customer name, address, telephone number and prescription medicine supplied.

"While he could not alter the prescriptions and we found no evidence that he disseminated the information, this constituted a serious invasion of privacy," said Stern.

After a plea bargain agreement, the juvenile will receive two years' probation, during which he may not possess or use a modem or other means of remotely accessing a computer or computer network directly or indirectly, must pay restitution to the telephone company and complete 250 hours of community service. And he has been ordered to forfeit all of the computer equipment used during the crimes.

Stern said: "This case reflects our intention to prosecute in federal court anyone, including a teenager, who commits a serious computer crime.

"The plea agreement is a balanced effort, weighing the seriousness of this juvenile's computer intrusions and his lack of malevolence. The freedom to explore with a computer and modem comes with the obligation to act responsibly and respect the law."

Analysis of the UK Police and Criminal Evidence Act, s.69 - Computer Generated Evidence - Part II

By
Amanda Hoey

In this second and final part of an article closely examining a crucial part of British law, Amanda Hoey looks at the issue of reliability and asks are the legal provisions really necessary.

Reliability

If there is a dispute as to the admissibility of a computer printout in a criminal case involving a jury, the judge should hold a voir dire. A party seeking to admit a printout under section 24 (or section 23) must establish the foundation requirements of both that section and section 69.

The judge, in deciding whether the prosecution has established these requirements, should apply the criminal standard of proof. (1) Although the additional requirements of section 69 can be proved by certificate, the foundation requirements of section 24 (or section 23) must be proved by evidence unless the other party makes admissions or allows the statement to be read.

There is also a third common law requirement, before the judge can decide on admissibility, namely that appropriate authoritative evidence must be adduced to describe the function and operation of the computer (eg R v Cochrane).

In R v Governor of Pentonville Prison ex p Osman [1989] 3 All ER 701 it was argued that printouts were inadmissible because the prosecution had failed to prove the proper operation of the computers required by section 69.

However Lloyd J held that "where a lengthy computer output contains no internal evidence of malfunction...it may be legitimate to infer that the computer which made the record was functioning correctly" (at p 727).

In R v Shephard the House of Lords held that it will very rarely be necessary to call an expert to prove that the computer is reliable. The defendant was charged with theft from a store.

A store detective gave evidence that she had examined all the till rolls for the relevant day from the tills, which were linked to a central computer, and that they contained no record of the unique product code for some goods found in the defendant's possession.

She also said that there had been no trouble with the central computer. On appeal it was argued that the evidence did not satisfy section 69 since oral evidence that the computer was operating properly is not admissible unless given by a person qualified to sign the certificate under para 8(d) of Schedule 3 which provides that: "In any proceedings where it is desired to give a statement in evidence in accordance with section 69 above, a certificate -....(d) purporting to be signed by a person occupying a responsible position in relation to the operation of the computer, shall be evidence of anything stated in it; and for the purposes of this paragraph it shall be sufficient for a matter to be stated to the best of the knowledge and the belief of the person stating it."

Dismissing the appeal, it was held that section 69 can be satisfied by the oral evidence of a person familiar with the operation of the computer who can give evidence of its reliability and need not be a computer expert.

Lord Griffiths said that: "Computers vary immensely in their complexity and in the operations they perform. The nature of the evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case. I suspect that it will very rarely be necessary to call an expert and...in the vast majority of cases it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly."

This approach was adopted in Darby v DPP The Times 4 November 1994. The appellant had driven her car into an area of road subject to a 30mph speed limit.

At that point a police speed trap was being operated. A police officer was operating a device known as a GR Speedman and he concluded that the appellant had exceeded the speed limit by driving at 43mph. It was submitted that the evidence of the reading of the GR Speedman was inadmissible if it was held to constitute a document.

It was also contended that the evidence of the read-out required certification and that, whilst oral evidence of certification would be admissible, the police officer could not give such evi-

dence as he was not an expert in the workings of the machine, only its operation.

Potts J adopted the approach of Lloyd LJ in the Shephard case and assumed that the machine was a computer and that the visual image was a document produced by a computer.

He also referred to the principle enunciated in Lord Griffiths' speech above and accordingly found no problem in holding that, on the basis of the evidence of the police officer, who was a trained and experienced operator of the device, the machine was working correctly. The appeal was dismissed.

Thus it seems that the provisions in section 69 are capable of being applied without undue difficulty. However, it is interesting to note that Rose LJ pointed out that if the GR Speedman had been central to this case and if it had produced a printout on which the prosecution had relied then it may well have been caught by section 10(1)(c) (2) of the Civil Evidence Act 1968 (section 118(1) of PACE 1984 provides that a 'document' within that Act has the same meaning as in Part I of the CEA 1968).

This would have meant that as a document within the meaning of section 10(1)(c) it would have constituted a document requiring certification within the meaning of section 69 and the terms of para 8 of Sch 3.

But it was the police officer's opinion evidence which was central to the case and that was capable of being corroborated by a technical device, the accuracy of which had been established.

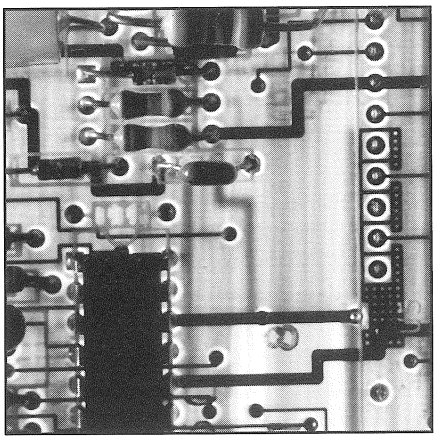
Thus it appears that the conditions for admissibility for computer output in a criminal case are less demanding if the evidence provided by the machine is merely corroborative.

The ambiguities and illogicality arising from the complex conditions for admissibility of computer evidence can clearly be seen in the recent case of McKeown v DPP [1995] Crim LR 69 where the Divisional Court held that if it cannot be proved that the computer was operating properly the computer evidence will be inadmissible.

This flies in the face of Lloyd LJ's dictum in the Osman case since the conclusion was reached despite the fact that evidence showed that the malfunction did not affect the accuracy of the information. The case concerned an appeal by Miss McKeown against her conviction for driving after having consumed so much alcohol that she was over the legal limit contrary to s 5(i)(a) of the Road Traffic Act 1988 and Sch 2 of the Road Traffic Offenders Act 1988.

The appellant underwent a breath test using the Lion Intoximeter 3000 breath testing device. This machine has a visual display and a memory which stores a number of results.

Four printouts were produced by the machine and these were certified by the officer in charge in accordance with s 69 PACE. On his statement the officer recorded the time shown on his watch as the machine was thirteen minutes out.



The submission of the appellant was that the visual displays and printouts were inadmissible on the basis that since the timing device was thirteen minutes slow it could not be shown according to s 69(1)(b) 'that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its 'contents'.

On behalf of the respondent it was argued that the words 'to a material degree' should be read into the statutory provision and that the incorrect timing did not in itself render the evidence from the machine de facto inadmissible.

Dr Williams, a director of the laboratories who supplied the breath testing machine, had been called as an expert witness on behalf of the prosecution. It was held that although he was not an electronics expert his qualifications and experience entitled him to give evidence in respect of the machine.

The court accepted his evidence that the working and accuracy of the breathalyser was not affected in anyway by the clock. However, despite these findings the court took the view that there was substance in the appellant's submission that on the wording of s 69(1)(b) the inaccurate timing mechanism on the machine rendered the print outs produced by it inadmissible.

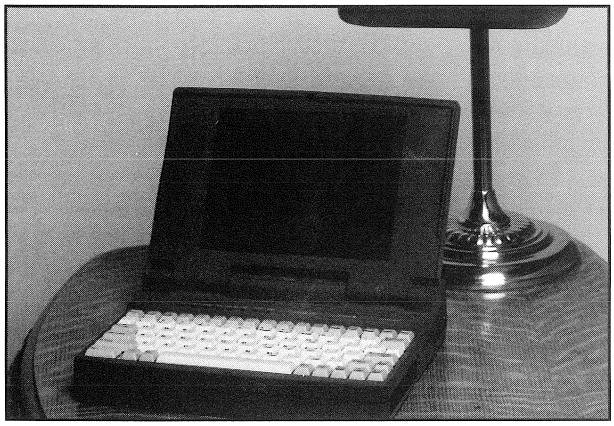
The appeal was allowed and conviction quashed wholly on the basis that, despite the evidence, the prosecution could not prove that the machine was working properly. The outcome, although in line with the statutory requirements of section 69(1) (b), is quite absurd since there was no question as to the reliability of the evidence.

The McKeown case also gives rise for concern in that the defence raised the smoke-screen of concentrating on the fallibility of the computer evidence rather than the reliability of such evidence. This point was raised by Dr Castell when he delivered The VERDICT Report to the Treasury in 1987. (3) He was perturbed that the current law could be effectively exploited by defence counsel to undermine a prosecution. The Law Commission in its Consultation Paper (Law Com CP No 138) claim that there is support for this contention in that judges commented on the lengthy cross-examination of prosecutions' computer experts.

It will be recalled that the standard of proof in a criminal case for evidence tendered by the prosecution is 'beyond all reasonable doubt'. The intricacy and complexity of many modern computer systems may make it relatively easy to establish a reasonable doubt in the juror's mind as to proper functioning of the computer.

Using the example of the McKeown case it appears that in the absence of a presumption that the computer is working means that it may be quite easy to raise such a smoke screen.

It would seem perfectly feasible that where there are doubts as to the reliable



reliability of computer generated evidence these doubts should not go to the issue of admissibility but rather to the weight of the evidence.

As we have seen in Shephard s 69 only applies where computer generated documents are tendered in evidence and there is an affirmative duty on those introducing computer evidence to show that at all times it is safe to rely on it.

Thus when applying a literal interpretation of the statutory provision illogicality and confusion reigns as demonstrated by the McKeown case. Furthermore it has been held that s 69 does not apply where a witness uses computer generated evidence to refresh his or memory nor where it is used by an expert to reach a conclusion.

In Sophocleous v Ringer [1988] RTR 52, another driving with excess alcohol case, evidence was given against the accused by an analyst who had used a computer which produced a graph illustrating the levels of alcohol in the blood stream. The graph was not put in evidence but the analyst was allowed to look at it to refresh her memory. As the graph had not been put in evidence the court held that s 69 did not apply.

The same outcome is illustrated in a recent Court of Appeal case, R v Golizadeh [1995] Crim LR 232. In this case a brown substance was found in the possession of the appellant which turned out to be a Class A drug (opium). The substance was analysed through a machine which produces a print out in the form of a pattern; this pattern is then interpreted by an expert to determine the chemical constituents of the substance.

In arriving at his conclusion that the substance was indeed opium the expert witness relied on his own interpretation of the print out and the opinion of another expert called to give evidence.

One ground of appeal was that under s 69 PACE the evidence should have been excluded on the basis that it was based on the computer print outs and was therefore inadmissible.

The Court of Appeal rejected this argument and held that s 69 did not apply. Morland J reiterated Lord Griffith's speech in the Shephard case whereby he stated that the object of s 69 "requires anyone who wishes to introduce computer evidence to produce evidence that will establish that it is safe to rely on documents produced by the computer".

Thus it is clearly the case that s 69 will only apply where computer print outs are actually put in evidence. Since in the present case the print outs had merely been used by the experts in reaching their findings as to the chemical constituents of the substance s 69 had no application on the facts of the case. In the words of the Law Commission in its recent Consultation Paper "if it is safe to admit evidence which relies on and incorporates the output from the computer, it is hard to see why that output should not itself be admissible" (Law Com CP No 138, para 14.13).

The irony of the situation is that it appears perfectly acceptable for evidence to be adduced which is based on computer generated print outs, but at the same time, if the computer evidence itself was to be presented to the court then the hurdle of complying with s 69 would have to be surmounted.

Are the special provisions necessary?

As we have seen, the statutory provisions impose special conditions on the admissibility of computer output. Are these justified? What is it that is special about computer-generated documents and that distinguishes them from their paper equivalents?

It is obvious from examination of the admissibility requirements that computer evidence is regarded as suspicious in several respects.

The main problem is concerned with the authentication and accuracy of computer records. It is almost as if the technology is believed to be inherently inaccurate. (4) Section 69 PACE requires some minimum proof of accuracy before the document is admissible. The court must be satisfied of the reliability of the statement as a true record of what the witness observed and also of its authenticity as an accurate record of what was intended to be recorded.

As a result it is necessary to show that at all material times the computer had been functioning properly, or at least that any malfunction had not affected the accuracy of the information.

It was envisaged by the Criminal Law Revision Committee (CLRC 1972, para 259) that there would be many cases where the document might have become corrupted by software errors or hardware malfunctions.

It is the contention of this article that this suspicion was probably unfounded on the basis that there has been no tangible evidence to date illustrating why computer records are likely to be less accurate than those contained on paper.

Paper based records are also susceptible to alteration and deterioration yet, where it is alleged that such alteration has taken place, the paper document remains admissible and the challenge goes to the question of its weight as evidence, to be decided on the basis of the evidence called to prove falsification or authentication.

Regarding documentary evidence para 3 of Schedule 2 to the Criminal Justice Act 1988 provides that: "In estimating the weight, if any, to be attached to ... a statement [given in evidence under section 23 or section 24] regard shall be had to all the circumstances from which any inference can reasonably be drawn as to its accuracy or otherwise".

Although no particular circumstances are specified, it seems safe to assume that regard may be had, for example, to the following matters: whether the person who made the statement in a

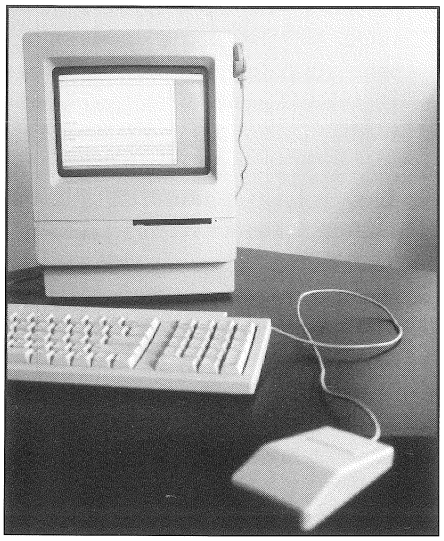
reliable document did so contemporaneously with the occurrence or existence of the facts dealt with in the statement; whether any person who supplied the information did so contemporaneously with the occurrence or existence of the facts dealt with in that information; and whether or not such persons or the 'creator' of the document containing the information had any incentive to conceal or misrepresent the facts.

In stark contrast to this, unless it can be shown that there is no chance of unauthorised use of a computer system, or of system failure, the same document stored on computer is inadmissible under the additional requirements of section 69 PACE (eg McKeown v DPP).

Doubts concerning the accuracy of information recorded on computers apply equally to paper-based systems, as do those concerning authentication. As with paper records, the necessary degree of authentication can be proved through oral and circumstantial evidence, if available, or via technological features of the system or record. (5)

Although a paper document can be authenticated by its author appending a signature, various technical ways of authenticating computer records have also been suggested. (6)

These could include electronic signatures in the form of smart cards, PINS or passwords and, although arguably less secure than biometric systems such as finger and palm printing and retinal scanning, the fact that foolproof authentication of a computer record is rarely possible is no reason for imposing stringent conditions on the admissibility of computer evidence.



There appears to be no intrinsic reason why different rules should apply to different forms of record-keeping, particularly when there may be no obvious difference in the appearance between a document produced by a computerised word-processing system and one produced on an electric typewriter.

It is interesting to note that this strict dichotomy between computerised information and manually compiled documents is witnessed, not only in the law of evidence, but also in the area of data protection. (7)

There seems to be a fundamental flaw in the statutory provisions in that they concentrate on the question of admissibility and not reliability.

Analysis of section 69 PACE shows that by making the admissibility of computer output subject to conditions which are really concerned with the weight of the evidence, the UK legislation places a double hurdle in the path of the litigant. The legal system should be able to ensure that provably reliable computer-generated evidence can be used in judicial proceedings, yet it confronts us with formalistic rules which appear to ask the wrong questions and address the wrong issues.

Another flaw is clear in the interaction of the statutory provisions with the hearsay rule. Although it has been shown that computer documents are not necessarily hearsay, the approach of the English law has usually been to treat them as if they were by excluding them as evidence unless specified conditions are fulfilled.

Where relevant computer-generated evidence and, indeed, all documentary evidence is provably reliable, it should be admissible in all circumstances regardless of the hearsay rule.

This of course would necessitate solving the problem of what is acceptable as evidence of the reliability of the evidence.

Indeed in regard to the question as to whether special rules are necessary it is significant to note that in Scotland, New Zealand, America, Canada and some Australian states there is no separate regime for computer evidence.

These jurisdictions appear to cope well without any special statutory rules (Tapper 1987, p 84) and as we have already seen, the problems associated with section 69 would suggest that there is obviously a strong case for abandoning the special regime for computer-generated evidence.

The Law Commission in its Consultation Paper (Law CP No 138) has suggested two options for reform; option one is to do nothing and option two is to repeal section 69 and leave it to the common law, relying on the presumption the machine works.

It is the contention of this article that option two is preferable for the reasons discussed.

Conclusion

It is imperative that the law should give industry and commerce clear guidance on how to make their records acceptable to the courts (see further Miller 1990; Bradgate 1990).

As technology develops evidential practice will need to be evolved to accommodate it. It is arguable that the judiciary themselves might be able to rescue litigants from some of the problems created by the special regime (as in the Osman case) but traditionally the law lags behind technological development.

If there were no pre-conditions for the admissibility of computer generated evidence then litigants could rely on the presumption of regularity whereby it would be presumed that the machine was working properly unless there was evidence to the contrary.

If this was the case the prosecution would not be under an 'affirmative duty' to lead evidence that the computer was working properly and would consequently avoid the problems faced by the prosecution in cases like R v Cochrane and McKeown v DPP.

It is the contention of this paper that there appears no good reason for treating computer records differently from paper documents and the rules, based on false assumptions about the technology, only create anomaly and confusion.

Forensic Q&A

Bibliography

Bradgate, R (1990) 'The Evidential Status of Computer Output' 6 Computer Law and Practice 142.

Criminal Law Revision Committee Eleventh Report (1972) Evidence (General) (London: HMSO) Cmnd 4991.

Keane, A (1994) The Modern Law of Evidence (London: Butterworths).

Law Commission Consultation Paper No 138 (1995) Evidence in Criminal

Proceedings: Hearsay and Related Topics (London: HMSO).

Miller, C G (1990) 'Computer-generated evidence - implications for the corporate user, Part 1' 6 Computer Law and Practice 178.

Nyssens, P (1993) 'The law of evidence:on line with the computer age?' (1993) 15

European Intellectual Property Review 360.

Reed, C (1993) 'Computer records as evidence-back to the beginning?' Journal of Business Law 505

Tapper, C (1987) The VERDICT Report.

Tapper, C (1989) Computer Law (London: Longman).

Tapper, C (1990) Cross on Evidence (London: Butterworths).

Tapper, C (1993) 'Evanescent Evidence' 1 International Journal of Law and Information Technology 35.

Footnotes

(1) R v Minors; R v Harper [1989] 2 All ER 208 (CA) at p 214. The standard of proof for the defence, presumably, is on the balance of probabilities.

(2) Section 10 (1) provides that:

"...document includes, in addition to a document in writing-...

(c) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom...."

(3) This report addressed the legal admissibility of digitally transmitted and processed data and information in the UK.

(4) There has been no documented research that I am aware of to support this view but the question to be posed is why else do the statutory provisions concern themselves with the accuracy of the computer- generated documents?

(5) See R v Shepherd [1993] AC 380 and Darby v DPP, The Times 4 November 1994.

(6) For a more detailed discussion see Heinriksen, 'Signature and Evidence' (UNECE doc TRADE WP.4/R98) in Legal Acceptance of International Trade Data Transmitted by Electronic Means, Special Paper No. 3 NORDIPRO, Universitets Forlaget., 1983, pp 40-101; and Reed, 'Authenticating Electronic Mail Messages - Some Editorial Problems' (1989) Modern Law Review 649.

(7) The Data Protection Act 1984 applies only to computerised information.

The author, **Amanda Hoey**, LLM, is a lecturer in law at the University of Ulster at Jordanstown, UK, and can be reached on e-mail at ahoey@ulst.ac.uk

This article was first published in the Web Journal of Current Legal Issues in association with Blackstone Press Ltd.

Q I have been hearing a lot about DVD drives being the coming technology. What are these and are they suitable for forensic use?

A DVD stands for Digital Video Disk or Digital Versatile Disk and are presented as a natural successor to CD-ROM technology. CD's have been with us a long time now and they were originally developed for digital audio use.

CD-ROM disks are cheap to produce, have a universally accepted standard format and the drives needed to access them are widely available and cheap to buy.

Later developments made it possible for special CD-ROM disks (known as CD-RW) to be written on ordinary Personal Computers (with appropriate hardware) and they are now in widespread use.

Unfortunately there are disadvantages - the amount of data that a single CD can hold is limited to around 680Mb, the media may be subject to degradation over time (so-called laser-rot and bonding breakdown) and is intolerant of heavy handling.

Small areas of bit corruption are not a problem when using CD's for digital audio but can be disastrous when storing digital data.

DVD technology uses improved materials and can contain (currently) up to 5.2Gb of data per disk. DVD-ROM and DVD-RAM disks are becoming available at reasonable prices and according to the industry pundits, this technology is expected to replace CD-ROM within the next two years.

Since the development is being driven by the entertainment industry (films and computer games) this seems more than likely.

They are superficially similar to CD's but the laser used is of a much shorter wavelength and capable of much finer focusing. This enables more than one layer of a disk to be used and correspondingly more data can be stored.

More details on DVD technology (and further links) are available on the Internet at http://www.cd-info.com.

Storing information for forensic purposes requires that consideration be given to the reliability, capacity, cost and speed of access of the media in question. For example, magnetic storage (particularly on tape) may degrade more rapidly than optical storage.

CD's are undoubtedly the cheapest form of storage but they are slower, smaller and less resilient than magneto-optical or phase change technology. This doesn't disqualify tapes or CD's from forensic use as long as the appropriate precautions are taken.

Whether the media is read-only or read-write is irrelevant except that rewritable media can obviously be reused.

With the increasing quantity of material being examined forensically, the size and speed considerations become more important and the expected 17Gb capacity of double-sided, multi-layered DVD disks appears very attractive.

If DVD provides acceptable levels of cost, speed and reliability, this increased capacity would seem to make it ideal for forensic use. No doubt the manufacturers of the various forensic copying systems are looking at DVD as an upgrade option and will conduct tests to determine its overall suitability.

E-mail questions, comments or suggestions, to the Journal at ijfc@pavilion.co.uk

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

Events

Proving computer crime: a master seminar

29 May 1998,
London School of Economics

Admissibility, Experts and Presentation. The LSE's Computer Security Research Centre and Queen Mary and Westfield's Computer Related Crime Research Centre are running a one-day Master Seminar on the following topics: Role of and instruction of experts; Types of evidence, practical issues of collection, provenance and formal procedures; Admissibility of evidence; Court presentation; Matters for Officers of the Court.

Each themed 45-minute session will be introduced by one or more individuals with specific experience but thereafter it is hoped that discussion will be extensive and open.

The numbers of attendees will be restricted so that an appropriate seminar atmosphere can develop. It should be noted that this seminar is designed for experienced practitioners, lawyers and law enforcement officers.

A summary of an illustrative case-study will be supplied to delegates to provide a focus for the day.

The seminar qualifies for 5 hours' of Law Society Continuing Professional Development

Contact: Lorraine Mulpeter, Centre for Commercial Law Studies, Queen Mary and Westfield College.

Tel: +44(0)171 975 5326
Fax: +44(0)181 980 2001

DIBS® User Group

30 April-1 May 1998
Newcastle, UK

Contact: Dave Lattimore
Tel: +44(0)1189 504611

Investigating computer crime and misuse: a one day training course

3 June 1998, London

This is an intensive training course aimed at auditors, IT managers and corporate security personnel. The object of the course is to train participants to respond effectively to a suspected fraud or incident within their own company where computer evidence will need to be secured and examined.

Contact: Catrin Jones,
Network International Ltd

Tel: 0171 344 8100
Fax: 0171 344 8101

First Joint British Congress of Forensic Sciences

8-12 July 1998, Glasgow

The Congress will be run under the joint auspices of The Association of Police Surgeons, British Academy of Forensic Sciences, British Association in Forensic Medicine, British Association in Forensic Odontology, The Forensic Science Society and Scottish Medico-Legal Society.

The meeting will cover a wide range of subjects of forensic interest.

Contact: Mr B Stewart, Dept. of Forensic Medicine and Science, University of Glasgow

Tel: 0141 330 4574
Fax: 0141 330 4602

Internet security and audit Workshop

17-19 August 1998, Bristol, UK

This workshop offers hands-on access to the Internet through a network of TCP/IP based servers and workstations. Learn how risks unfold as new technologies evolve; how to detect weaknesses, control access and protect sites from security breaches. Learn about firewalls and secure gateways and how to review network security. Use special network review software and examine some of the hackers' tools.

Contact: Margaret Mason

Tel: 01625 523205
Fax: 01625.526952

Published by
Computer Forensic Services Ltd.