ISSN. 1363-6650

JULY 1997
Issue 7

International Journal of FORENSIC COMPUTING™

Contents

Editorial Team

- Paul Johnson
  Editor
- Sheila Cordier
- Jo Collard
  Design & Layout

Comment

Like the birth of any new technology, the Internet needs to be closely watched to make sure it works for rather than against society. Like a child, it has to be pointed in the right direction, even if that means the occasional reprimand, and it has to be able to work within the framework set by that society so that it does not pick up bad habits or become malicious.

But give it a free run and it will become a spoilt brat, resenting any form of control and unable to exercise self-restraint.

Many of those who had followed the case of the Communications Decency Act in the US greeted its demise with unbridled joy. The axing of the legislation was for some the "birth of the Internet" and they claimed that freedom of speech had triumphed over gross intrusion by the state.

True, the CDA contained many inconsistencies and was too vague to have any practical use in the real world. It was, at best, a brave but foolhardy attempt to protect people from the worst excesses of the Internet and acted as a warning about the sheer power that electronic communications can bring.

The number of people using the Net is expected to mushroom to 200 million by 1999, with the number of web sites and variety and level of information available rising correspondingly. Make no mistake, this is not a techno-nerd's plaything but probably one of the most important communication and resource facilities available.

Broadcast and print media in most countries is controlled and has to abide by certain taste and decency standards, but who patrols the Internet? It is certainly true that illegal and irresponsible material, such as hardcore child pornography, hackers' handbooks and terrorism information, are all available on the Web if you know where to look.

Perhaps some of those who whooped with joy as the CDA was struck down would be somewhat more subdued if they found their ten-year-old son downloading porn or communicating with a paedophile over the Net.

One man's freedom of speech is another's violation of moral standards and the crossover between the two is very blurred. Yet there are basic standards which any modern society or state can expect, and it is these that have to be safeguarded.

The bottom line is that there has to be some form of legislation so that law enforcement agencies can go about their job. Already Germany has taken a strong line and is vigorously investigating and prosecuting suspects in its own territory.

But the US's recent experiences will cloud the issue internationally, and could set back Internet law by several years. Because the Web cuts across any physical or geographical boundary or border, it needs a global approach as to what is acceptable and how it will be enforced. Many critics say normal laws cannot work in cyberspace, but that is wrong. The legislation just has to be sensible and practical.

It is very early days yet and the Internet is just in its infancy. With a bit of gentle coaxing it will grow up into a responsible and effective system.

The Journal would welcome letters or feedback on any issue of forensic computing. Send your letters by e-mail, fax or post to the address on this page. ■

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

Articles are published on the understanding that publication is not taken to imply endorsement of the views therein by the Publisher or Editorial Team or members of the Advisory Board of the Journal. Courses of action described in the Journal in relation to one set of circumstances will not necessarily be appropriate for a different set of circumstances.

Accordingly, readers should take their own independent specialist advice before proceeding on any project or course of action and any failure to do so is at their own risk. No responsibility is assumed by the Publisher or Editorial Team or members of the Advisory Board for any loss or damage to persons or property as a matter of contract, negligence (save in respect of liability for death or personal injury arising out of any negligence) or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Whilst all reasonable care is taken, neither the Publisher, nor the Editorial Team, nor members of the Advisory Board can be held legally responsible for any errors in articles or listings. Upon submission of an article, the author will be requested to transfer copyright of the article to the Publisher.

News

Cyber crime seminar

Top law enforcement agencies and online service providers came together to discuss how offences committed on the Internet can be investigated and prosecuted.

The event, held in New York, US, looked at issues such as child pornography, consumer fraud, hacking, online harassment and viruses, and examined the methods and legislation used to catch suspects and take them to court.

New York State Attorney General Dennis Vacco said: "I am committed to making sure that crimes, no matter what medium they may occur in, are investigated and prosecuted. The seminar is just one of many steps my office is taking to ensure that consumers are safe in cyber-space."

Investment in crime fighting

An Australian police force is buying hundreds of new PCs as part of a A$ 2 million restructuring process to make it more effective.

The New South Wales State Police will get an extra 500 PCs, worth A$850,000, as well as another A$1 million to buy printers, faxes, radios and a satellite communications system.

State police minister Paul Whelan said the move would give the police on the frontline the necessary tools to tackle critical high crime areas.

Online banking warning

The Bank of England has told investors to carefully check an Internet banking service before making any transactions.

It said it was difficult for customers to tell where a bank offering service online was based, or whether it had approval in the UK or abroad.

A report said: "The Bank advises anyone responding to advertisements for deposits placed on the Internet to check whether or not the bank is properly authorised."

Hacker charged with theft

The FBI arrested a 36-year-old man in connection with a scheme to steal more than 100,000 credit card numbers from online companies.

The man, from Daly City in California, US, is alleged to have rigged up a credit card number packet sniffer by using existing technology and adding to it with his own inventions.

It was only when the sniffer was found on an internet service provider's server that the FBI set up a sting operation with a false buyer to catch the suspect.

An FBI spokesman said: "If this individual can do this, how long is it going to take before someone else tries to. That is one of those scary questions."

Gambling on the Web

Workers who use the Internet to gamble are costing businesses time and money, according to an industry thinktank.

The Masie Centre in the US, a technology consultant, says there are dozens of betting sites on the Net and that bosses could be unaware of what is going on under their noses.

Director of the firm Elliott Masie said: "Human resource managers should take a quick look at the gambling sites and integrate a policy into their employee handbooks as well as restrict access.

"It is also an area of ambiguous law as most states don't regulate the new innovation and it is even unclear where the potential offence is taking place."

Technology used in Mafia crackdown

New computer systems are being used by tax authorities in Italy to search and cross reference the records of crime bosses.

Prosecutors are using the information to fight the Mafia by removing its wealth and taking away its property and businesses.

The system was used to confiscate a $1.2 billion empire built up by one of the top men, who in 1989 had declared an income of just $1,100.

French with tears

The Canadian province of Quebec is warning businesses using the Internet to comply with strict language laws or face stiff fines.

Under Quebec legislation, commercial publications have to be in French and the authorities say this also includes any web sites or advertising on the Net.

Firms breaking the regulations could be fined up to $1,400, despite a statement by the Canadian heritage ministry that telecommunications are a federal and not provincial issue.

Indecency law blocked by judge

Legislation to crackdown on Internet paedophiles was stopped by a US federal judge because of fears it was too localised.

The New York law introduced nine months ago made it a crime to send sexually explicit material to children via a computer and those caught could have faced up to seven years in prison.

Now US district judge Loretta Preska has issued an injunction to block the legislation and said that the law was well intentioned but unconstitutional.

She said: "The protection of children from paedophilia is an entirely valid and laudable goal of state legislation. However the New York act's attempts to effectuate that goal fall foul of the federal Commerce Clause."

A spokeswoman for the American Civil Liberties Union, which had filed to have the law overturned, said: "This is an important victory. It sends a really strong message out to state legislatures that you can't pass laws to censor the Internet."

In a similar case another federal judge in Atlanta rejected a Georgia state law aimed at fighting fraud that banned anyone sending anonymous communications over the Internet.

Judge Martin Shoob said the law would ▶

harm people who have legitimate reasons to remain anonymous, including those who wanted to maintain privacy or feared discrimination or harassment.

In a decision which may set the tone for global Internet law, the US federal Communications Decency Act was struck down. See page 6 for details.

Stolen antiques sold on the Net

Italian Police have arrested a man suspected of using the Internet to advertise and supply antiques worth millions of pounds.

The 59-year-old man, a painter from Northern Italy, is alleged to have obtained the priceless artefacts from important archaeological excavations and put details and pictures of them on the Web.

Ancient objects on the site at http://www.webstore.fr/archeo included a seal dating from 2,500 BC, a stone Phoenician cat and a bronze Roman dolphin.

Captain Antonio Del Gaizo, commander of the finance police unit at the Italian town of Susa, said: "As far as I know this is the first case of its kind, but it could be just the tip of an iceberg."

Police plan to use the Internet to fight back by posting a catalogue of stolen artefacts on the Web as a guide to other law enforcement forces, dealers and auction houses across the world.

Swiss woman in Internet porn case

A woman who used the Internet to send child pornography pictures to a friend has been sentenced in the first case of its kind in Switzerland.

The court in Lausanne heard that the 33-year-old woman, who was given a 15-month suspended sentence, had been living in the US since 1993 and sent about ten paedophile images across the Net to Switzerland.

Investigators discovered the illegal pictures by accident while they were looking for software piracy on seized computers from the woman's friend and they used e-mail records to track the woman down.

Hacker banned from computers

Convicted hacker Kevin Mitnick has been told by a US federal judge to keep away from all computers, mobile phones and software when he is released from prison.

The order came as Mitnick, 33, was sentenced to 22 months in prison for possessing illegal cellular phone codes and for violating his parole. He was also banned from being employed in any job that would allow him to have access to computers without approval from the probation service.

Mitnick admitted last year to possessing fraudulent phone codes that let him access cellular phone networks and the crime happened while he was on parole for an earlier hacking offence.

Germany passes law for Net control

Pornography and Nazi propaganda on the Internet have been banned under a new German law which comes into force on August 1.

The legislation means Net providers can be prosecuted for offering a venue for illegal content, even if it came from beyond German borders, if they do so knowingly and that it is "technically possible and reasonable" to prevent it.

German research and technology minister Juergen Ruettgers said: "The Internet is not outside the reach of the law. That applies even to a network that knows no national borders."

Prosecutors in Germany have been at the front of the movement to police the Web, with the indictment of CompuServe's German manager Felix Somm who has been charged with knowingly allowing pornographic pictures to reach its customers.

The legislation also makes Germany the first country to set rules for digital signatures so that authenticated financial transactions are secure and legally binding under banking law.

Meanwhile a left wing German politician who was accused of supporting terrorist acts with Internet information has been acquitted by a Berlin court.

Angela Marquardt, 25, a former deputy leader of the Party of Democratic Socialism was alleged to have used a hypertext link from her home Web page to an Internet magazine which described how to sabotage railway lines.

The Radikal publication, which is based in the Netherlands, is banned in Germany and gave advice to anti-nuclear activists.

But the court heard that Marquardt had installed the link before the magazine had published the instructions and ruled that she could not be held responsible.

Net in fight against drugs

Police from seven South American countries are using the Internet to step up their campaign against narcotics traffickers.

Law enforcement intelligence officers will use an encrypted website to share information on drug gangs and bosses. The site will also pinpoint the location of illegal drug labs, illicit coca and opium poppy crops and alert the authorities to cross-border movements.

Col Oscar Naranjo, intelligence chief of Colombia's National Police said that the idea of using the Net came after finding out that the drug barons were using it themselves to co-ordinate their activities.

He said: "Various clans dedicated to drug trafficking and organised crime are using top-notch tools."

Call for ban on Net porn

A Sentate select committee said that Net users should conform to the same laws as any publisher or advertiser in Australia, but both Labour and Australian Democrat politicians rejected the ban, saying that the issues were too complex. The committee wanted to make it illegal to use computers to transmit, obtain, request or advertise some material, including pornography and anything that promotes criminal activity. ■

Product News

Learning machines help police

Automatic recognition specialist Neurodynamics is expanding to meet new demand from police forces and government offices across the world.

The firm, with bases in the UK and US, already has systems such as fingerprint and face recognition, fraud detection and data mining. It is now launching into new areas, including biometrics, advanced database technologies, vision and imaging and intelligent character recognition.

Managing director of Neurodynamics Dr Michael Lynch said: "The remarkable thing about neural network technology is that it is a learning technology. The same basic system can learn to tackle any number of different real life problems.

"Our success generates a need for specialist groups to focus on particular application areas in order to optimise product development and strengthen the partnership with our customers."

Neurodynamics can be contacted on +44 (0)1223 421107, e-mail esbneurodynamics.com and more information is available on the web site at http://www.neurodynamics.com

New fingerprint system

A state-of-the-art automatic fingerprint system will help catch criminals and keep prisoners behind bars.

Atlanta police department together with the state's department of corrections hopes to have more than one million people on the new fingerprint database system by early next year.

Its maker, NEC, says the automated fingerprint identification system will give accurate suspect identification, streamline records and ensure that close tabs are kept on all inmates as well as controlling inmate movement between prisons.

Atlanta police department chief Beverly Harvard said: "The technology involved in crime and particularly in crime prevention, is rapidly changing and we must build solid systems today if we are to meet the challenges that we will encounter in the future."

More information about the NEC system can be found on the web at http://www.nec.com/afis

Data retrieval application

Excalibur Technologies has launched a new unit called the Visual Business Group to handle its information retrieval development.

The new branch will be responsible for the US firm's Visual RetrievalWare system, which helps find and access digital information, including fingerprints, signatures, photographs and videos.

Using recognised patterns in digital code, the program can analyse, index and retrieve images based on specific visual content.

Contact +1 703 761 3700 or e-mail: ccromleyexcalib.com

Law web site

An Internet site set up by Legal Data Search Inc helps users find information online about the legal profession.

The pay-to-access site is based on a large database and has a search engine to look for specific topics and detailed requests.

Users pay $10 for a two hour session on the site, which is at http://www.legaldatasearch.com

Secure networks contract

US firm Infringatek Inc announced it has won six contracts to build secure computer networks for legal firms in the Washington DC area. The company says the communications have to be totally tamper proof to prevent sensitive information leaking out.

Infringatek president Sudeep Bose said: "Secure systems and private communications are imperative to attorneys in order to protect the interests of their clients. With the increased use of e-mail and remote communications you have to pinpoint and patch-up weaknesses or face the uncertainty of malpractice suits.

"Many of our security people were investigators in the past. They were the ones chasing hackers and investigating holes in various systems. They know the tricks of the trade and what it takes to protect our clients."

Details of sex offenders

People living in California in the US can check up on whether they have a convicted sex offender living in their neighbourhood.

San Diego company Epic Solutions Inc is providing software to the state's department of justice to create a CD-ROM database giving detailed information on more than 63,000 registered offenders.

California is the first state to set up such a system, although it is thought that others will follow. Files available to the public include an offender's name, photo, post or zip code, identifying marks and some previous convictions.

Chief executive officer of Epic Solutions Dan Crawford said: "This is a major step forward in providing the public with a powerful weapon to help defend themselves and their families against predators. This very well could be a prototype for use across the US."

The legislation which allows citizens to see information on sex offenders is known as Megan's Law after Megan Kanka, the seven year old girl who was raped and murdered in New Jersey in 1994 by a twice-convicted sex offender who lived in the same street.

Exception to encryption exports

The US Government will bend export rules and allow Microsoft and Netscape to sell their most sophisticated data scrambling technology to overseas banks.

The companies are currently banned from selling encryption software abroad because of fears that the programs may be used by criminals to commit cyber offences.

But banks are thought to be a safer bet as regulations require them to keep detailed records of transactions and the technology is tightly controlled. The encryption facility is used in versions of Internet browser software ▶

so people can make secure online transactions.

Mitchell Baker, from Netscape, said: "We have had a huge number of our current and potential banking customers overseas tell us this is critical to banking applications outside the US."

The approval comes as the computer industry in the US pushes to have the regulations relaxed as they fear firms elsewhere in the world have a commercial advantage.

Computer security systems

UK firm Dalen is supplying a range of physical security products to minimise the risk of unauthorised access or theft.

The company has computer safes, desktop cages and special cables to fit most needs and it says laser printers, faxes and monitors can also be protected easily.

Contact Dalen on +44 (0)121 428 1133

New security strategy

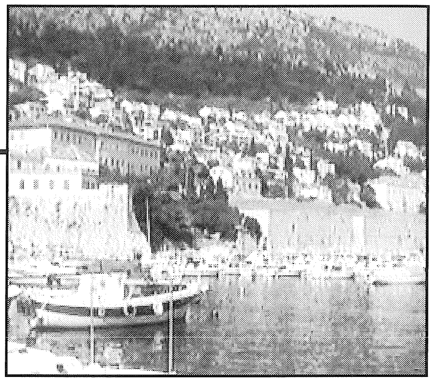
Sterling Commerce in the US has launched a package of security measures designed to help businesses reduce the risk of online crime.

The firm, which has offices across the world, announced new encryption and firewall software to make sure that communications or financial transactions of the Internet or over an intranet will be free from hackers or other prying eyes.

Sterling Commerce spokesman Steve Perkins said: "With conservative industry estimates marking financial losses from computer crime at more than $10 billion a year, this is an invaluable tool to organisations requiring information confidentiality. Not only does this software offer next generation encryption for file, memory and streams based data, the simplicity of the desktop application makes it usable by anyone."

For more information contact Sterling on +44 (0)181 867 8000 or e-mail on john—kharaystockley-park.sterling.com ■

Croatia -



Computer Crimes Conference

In June, the conference room on the top floor of the Hotel President in Dubrovnik played host to Croatia's second International Computer Crime Conference.

The audience of more than 150 judges, lawyers, public prosecutors, academics and law enforcement officers were eager to learn of the latest practical developments and legal procedures in the collection, examination and presentation of computer based material in criminal investigations.

From the entrance to the conference room we could look out and see a handful of the emerald islands set in the azure Adriatic. With temperatures in the 30's and such a setting it was hard to imagine the issues that were to be presented and discussed in that shaded conference room.

The conference was aimed at raising international awareness of computer crime, addressing some of the issues that affect law enforcement and judiciary. Seventeen central and eastern European countries were invited to attend which gave the audience a truly international flavour. A popular delegation from the Ukraine had journeyed for three days by train to attend because of the higher cost of flying. This dedication and endurance typified the feeling within the audience as to how important this conference and these issues really were.

The conference was opened by the Assistant Minister for the Interior followed by short addresses from several senior members of the Ministry. Guest speakers from the UK included His Honour Judge Rivlin QC and Simon Dawson, a senior member of the Crown Prosecution Service. Both presented aspects and procedures on UK law relating to the prosecution of computer criminals, referring to a variety of computer cases that they had dealt with.

The backbone of the conference was a series of lectures from Simon Janes and Mark Morris, both experienced members of Scotland Yard's Computer Crime Unit. They dealt with various facets of computer crime, always with the emphasis on practical issues and with lots of case history material.

Reflecting the lead which the UK has in the field of computer crime, two civilian experts from England had also been invited to address the conference. Paul Holroyd of i2 Limited gave a presentation on his company's analytical software and was received with great interest as he discussed how best to analyse the vast amounts of data which computer crime investigations can generate.

Jim Bates of Computer Forensics Ltd presented sessions in which he discussed first the practical problems of securing and collecting data using the DIBS© system and then investigating and analysing it on dedicated forensic workstations with specially written software. His final presentation dealt with the problems and solutions highlighted by selected case histories.

A final, lively question and answer session was ably chaired by Ognjen Haramina of the Croatian Economic Crime Department and included Simon Janes, Mark Morris and Jim Bates on the panel. This was reluctantly drawn to a close after an hour but the quality of the questions and discussions during that time amply demonstrated the interest and attention of all delegates throughout the week. After the closing speeches and as the delegates made their goodbyes, the general opinion among both the locals from Croatia as well as many others from such countries as the Ukraine and Slovenia was that for once this was a conference that had really achieved something constructive.

Simon Janes, in his closing address had quoted Chairman Mao who said, "A journey of a thousand miles begins with the first step". Delegates and expert speakers alike undoubtedly left feeling that first step had been made and the journey was well and truly under way. ■

Internet Law

One of the most important pieces of Internet crime legislation was thrown out in the US for being unconstitutional. Paul Johnson looks at the case and the implications it has for drafting computer laws.

In one of the most controversial decisions on computer crime, the Communication Decency Act has been struck down because of fears that it violated free speech. In its first venture into Net law, the US Supreme Court decided that the legislation restricted citizens' rights to communicate.

The law, which was passed by Congress in 1996, was aimed at protecting children from indecency online and banned adult material and pornography which could be easily accessed by minors.

It made it a crime to put offensive words or pictures on the Net where they could be found by children and offenders faced up to two years in jail and a $250,000 fine. Under the legislation, adult material could still be put online if it was accessed only by credit cards or special access codes, but there were no restrictions on pornography sent from computers on the Web outside of the US.

But the CDA was challenged by a variety of groups including the American Civil Liberties Union, America Online, Apple Computer and the American Society of Newspaper Editors, who said the law would restrict the discussion of sensitive and important issues.

The court found there was no practical way to regulate indecency online without radically altering the First Amendment rights of adults, so that the CDA would have reduced the Internet to a uniform child's level.

Writing for the court, Justice John Paul Stevens said: "The Internet constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers and buyers. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox.

"It is true that we have repeatedly recognised the governmental interest in protecting children from harmful materials. But that interest does not justify an unnecessarily broad supression of speech addressed to adults. The Government may not reduce the adult population to only what is fit for children."

He added: "We have remarked that the speech restriction at issue amounted to burning the house to roast the pig. The law casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community.

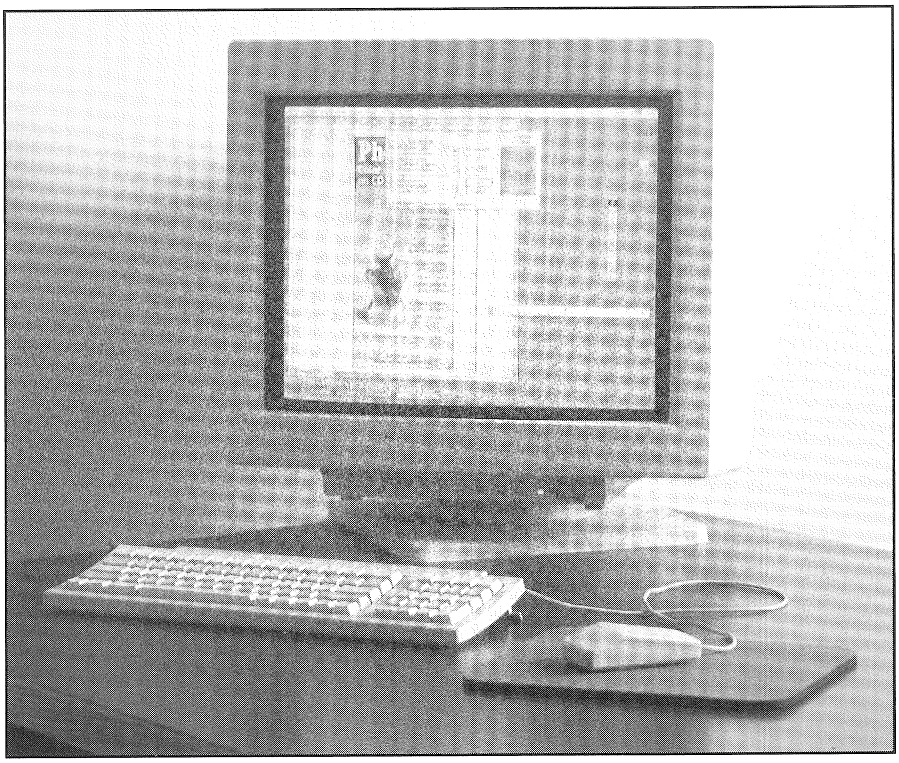
"The CDA is akin to a law that makes it a crime for a bookstore owner to sell pornographic magazines to anyone once a minor enters his store...the absence of any means of excluding minors from chat rooms in cyberspace restricts the rights of adults to engage in indecent speech in those rooms."

In the ruling, the justices said that any restrictions on access should be at the customer's end with software filters rather than laws being used to shield children away from pornography, unpleasant pictures or adult chat.

The Supreme Court recognised that the CDA was seriously flawed in two main areas. Firstly it was too vague and could stop lawful communications because of fears of criminal sanctions, and secondly it did not take into account the global scale of the Internet, which knows no frontiers or political boundaries.

Logically it should be easy to ban the sale and distribution of pornography to children on the Internet, but the CDA failed essentially because normal terrestrial laws cannot be made to work in the same way in cyberspace.

Legislation based on broadcast standards of indecency are irrelevant because the Internet works on a request basis, with users voluntarily accessing certain pages, unlike the television and radio which are considered invasive. Laws banning indecency must define exactly what indecency is, which was a major stumbling block for the CDA. And laws banning indecent communications with minors are unworkable because users never ▶



know for sure who else is under the age of 18.

Sen Patrick Leahy, one of the leading opponents of the CDA, said: "This decision is a landmark in the history of the Internet and a firm foundation for its future growth. The Communications Decency Act was misguided and unworkable. It reflected a fundamental misunderstanding of the nature of the Internet and it would have unwisely offered the world a model of online censorship."

But supporters of the CDA now fear the ruling will harm parents' ability to guard against pornography and reduce the power of law enforcement agencies to investigate suspects.

Sen Dan Coats, who sponsored the law, said that the justices were "telling parents to abandon any hope of a decent public culture".

Pat Trueman, director of government affairs for the pro-CDA American Family Association said: "The ruling was regrettable, but it doesn't mean that pornography has to flourish on the Net.

"The CDA only deals with soft-core pornography, not hard core pornography that's considered obscene. If the Justice Department was serious in prosecuting obscenity and child pornography, people wouldn't be talking about the CDA."

Cathy Cleaver, director of legal policy at the Family Research Council in Washington, said: "As of today, the floodgates are open and pornographers can invite children in. But we're not going to stop fighting for protection for kids online. We will go back and you will be seeing a more narrowly drafted statute."

President Clinton, who has been uncommital on the CDA affair, said: "The Internet is an incredibly poweful medium for freedom of speech and freedom of expression that should be protected. But there is material on the Internet that is clearly inappropriate for children. We must give parents and teachers the tools they need to make the Internet safe for children.

"With the right technology and rating systems, we can help ensure that our children don't end up in the red light districts of cyberspace." ■

Internet Sites

Computer investigators have many tools at their disposal to copy and analyse information taken from a suspect's machine. One recent development is the ability to examine and collate evidence on the data's physical attributes to try to find something about its history on the computer.

The World Wide Web is an invaluable research tool for computer crime investigators, with an almost inexhaustible number of academic papers, articles, newsgroups and practical information and advice.

And investigators can make use of thousands of freeware and shareware files to be found on the Net which can make all the difference in an investigation. Here are a list of some of the sites available, along with short descriptions.

To access them, investigators need only a computer, modem and an Internet service provider. Most sites are best viewed using Netscape 3 or above or Microsoft Explorer 3, although other online viewers will work satisfactorily in many cases.

This list is by no means comprehensive and represents only a small number of useful WWW sites for computer investigators. Using the various search engines, such as Infoseek and Alta Vista, will produce many new leads.

If readers of the Journal know any useful WWW or FTP sites, please send them in or e-mail them to us and we will publish them for others to use.

Police and investigation

- **Police List of Resources at** *http://police.sas.ab.ca/prl/index.html*
  This impressive page does exactly what it says - it acts as an A to Z index listing everything from police dogs to firearms.
- **The electronic crime page is at** *http://police.sas.ab.ca/prl/elect.html*
  and features the work of the US Customs, Scams on the Internet and a terrorism issues page.
- **The High Technology Crime Investigation Association page is at** *http://htcia.org/*
  This gives details and contact addresses for members, information on courses and seminars and lots of links to other sites on the Web.
- **Cybercop at** *http://www.well.com/user/kfarrand/index.htm*
  This page has a somewhat "clubby" feel to it but does offer an "underground" opinion and has some very good links to other sites.
- **The FBI at** *http://www.fbi.gov/homepage.htm*
  This professional and comprehensive site includes everything from the US's most wanted fugitives to the Bureau's publications, offices, major investigations and case studies.
- **The FBI's National Computer Crime Squad page is at** *http:www.fbi.gov/programs/nccs/compcrim.htm*
- **The International Association of Computer Investigative Specialists at** *http://cops.org/*
  This gives details of membership, training, news and also has links to other pages. Most useful are the links to local and regional police forces in the US and elsewhere in the world.
- **Digital Crimes Investigation Network at** *http://www.schmidt.org/*
  This very useful site has a good list of related sites as well as technical advice and utilities for the investigator on Windows 3.1/95/NT and Macintosh systems. At the time of writing, two programs for Windows were available - one which allows read only access to a NTFS formatted partition and another which allows an investigator to browse through Netscape's cache directory and ▶

determine sites that were visited.

- **Royal Canadian Mounted Police at** *http://www.rcmp-grc.gc.ca/html/rcmp2.htm*
  This is an incredibly comprehensive website for a police force and includes just about everything about the Mounties, complete with a search facility. There is lots of information on computer crimes, with an excellent overview of the problem as a whole. Recommended.
- **American College of Forensic Examiners at** *http://www.acfe.com/*
  A useful and well-organised site, this lists membership details, courses and other links. This is of primary interest for mainstream forensics such as medical and ballistics, but has some useful information for computer forensic investigators.
- **Houston Area Technical Support at** *http://www.ghgcorp.com/cybercop/*
  HATS is an interagency group aimed at helping police and prosecutors to combat technical crime. The site has information on training, presentations and an extremely large software library for computer crime investigation at its bulletin board, which requires membership of HATS.
- **The National Institute of Justice Office of Science and Technology at** *http://www.nlectc.org/*
  Good for general information, with strong links as well.
- **US Department of Energy Computer Incident Advisory Capability at** *http://ciac.llnl.gov.ciac/CIACHome.html*
  This excellent site is of considerable practical interest to investigators and contains a wealth of technical advice on numerous operating systems and a host of varied utilities and applications.

FTP sites

These contain thousands of downloadable files and programs, many of which are of direct relevance to computer investigators. There are many sites around, with too many files to list.

ftp://wuarchive.wustl.edu/
ftp://ftp.uu.net/
ftp://oak.oakland.edu/
The vast amount of software in these sites can be a little overawing, but there are indexes and lists on each site which can help pinpoint relevant files.

Law

- *Online Law at www.online-law.co.uk*
  This is intended as a starting point for legal research in the UK and consists of a searchable database together with information on the Bar and the solicitors profession. Included are lists of lawyers, courts, expert witnesses, technology suppliers. Also includes more than 2,000 links to other legal pages on the Web.
- *SCL at www.scl.org*
  The Society for Computers and Law puts out this site, which includes diary dates of SCL activities, an online noticeboard and discussion chamber, an electronic magazine and information about other law groups.
- **University of Iowa Internet resources at** *http://www.lib.uiowa.edu/gw/journalism/mediaLaw/media-law.html*
  A good starting point for finding law articles and judgements on computer crime and prosecution. Mainly US focused, but huge in scope.
- **Computer crime research resources bibliography at** *http://mailer.fsu.edu/~btf1553/ccrr/books.htm*
  This is a useful list of books and publications covering all aspects of high technology crime and investigation, listing author, title and publisher. Only a handful of books are accessible online, but useful non-the-less.
- The full text of the publication **The Hacker Crackdown: Law and Disorder on the Electronic Frontier, by Bruce Sterling,** is available at *http://www.usfca.edu/crackdown/crack.html*
  The welcome section of the Computer Crime Research Resources site contains a large number of Net site listings, including various laws, codes of practise, cases and a searchable index.
- **Computer Professionals for Social Responsibility at** *http://www.cpsr.org/dox/home.html*
  A large site definitely worth having a look at, with a considerable amount of information, links and discussion material in the field of computers, law and ethics.
- **United Nations international review of criminal policy**, manual on the prevention and control of computer related crime at *http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html*
  The full and extensive text of this important document, split up into easily managed sections.
- **Computer Crime and Investigation Center at** *http://www.ovnet.com/~dckinder/crime.htm*
  Draws on many links to associated areas, particularly in the fields of security and preventative measures, and offers helpful advice on the issue as a whole and on specific details.
- **A Guide to Understanding Data Remanence in Automated Information Systems at** *http://www.ovnet.com/~dckinder/documents/darkgreenhtm*
  A document written by the US Department of Defense which looks at information stored on hard disks and how it can be erased or retrieved. ■

The above Internet sites represent only a tiny fraction of what is available. If any of the links are not working, please contact the Journal so we can alert readers. Similarly, if anyone knows of other useful sites or programs that can be downloaded, let us know and we will publish the details in the Journal. E-mail us at ijfc@pavilion.co.uk

Profile

Howard Schmidt

Howard Schmidt, Supervisory Special Agent, director of US Air Force Office of Special Investigations Computer Forensic Laboratory.

Ever since computers emerged as hobbyists playthings, Howard Schmidt has been at the forefront of high-tech investigations. His CV reads like a Boys' Own adventure book and he is currently helping to set up a computer crime laboratory for the whole US Defense Department.

Mr Schmidt has been with the USAF for about 19 years, including seven years active duty serving three tours in South East Asia, including Vietnam, Thailand and Korea, and he has also spent nine years as a Department of Defense civilian, serving as a chief of transportation and as a deputy director of resources.

He is currently a supervisory special agent, director of the Air Force Office of Special Investigations Computer Forensics Lab and Deputy Chief of Computer Crime and Information Warfare. Mr Schmidt came to the unit from the FBI at the National Drug Intelligence Center where he headed the Computer Exploitation team as a computer forensic specialist. Before that he was a police officer for 11 years and member of their SWAT team for nine years.

From 1986 to 1991 he worked in the criminal investigation division in the police department in Chandler, Arizona, and began to look seriously at the issues involved in computer crime. He said: "I'd always been involved in ham radio so when the first computers came out I naturally wanted to get involved. I bought one of the TRS-80s and it started from there. I used personal computers help investigate crimes as well as cases where violators used computers to store customer lists, drug ledgers and financial information."

In 1987 Mr Schmidt went on to teach a special course in Phoenix designed to instruct police officers advanced narcotics investigations including computer search and seizure techniques.

He is now a regular instructor for the National White Collar Crime Center, the FBI Academy and the USAF Office of Special Investigation and he is also an executive board member of the International Organization of Computer Evidence, co-chairman of the Federal Computer Investigators Committee and is a member of the American Academy of Forensic Scientists and the American Society of Crime Lab Directors.

Mr Schmidt is adamant that investigators have to keep on their toes with the latest developments in order to be efficient and effective.

He said: "It's hard to keep up with everything because technology is always moving on. The size of hard drives makes our job trickier. Now drives such as 2.1 GB or even bigger are common. At one stage DOS was the only operating system, but now we've got Windows 3.1, Windows 95, Linux, Windows, NT and Macs.

"We have to be prepared to investigate them all and use whatever techniques are necessary. It's very important to keep pace and to re-educate yourself, which is a continually ongoing process.

"I'm in regular contact with people across the world so I know what other investigators are doing. It's extremely important that we talk to each other and get ideas and information of each other, so we all don't end up reinventing the wheel all the time."

When the Department of Defense computer forensic laboratory project is complete, Mr Schmidt expects the team to be involved in about 500 cases a year. He said: "A lot of the procedures we have are automated, which means staff time can be better spent. At the moment the Air Force carries out investigations into both the military and civilians, with a broad range of cases.

"What is needed is more training. The investigators who can use computers to help solve crimes will be the investigators of the future. You don't have to be an expert, or know exactly how it works, you just need to know what it can do."

Mr Schmidt has processed computer evidence for the FBI, Drug Enforcement Administration, US Customs, US Postal Service as well as state and local police forces. The cases have included telecommunications fraud, extortion, narcotics trafficking, racketeering, murder, forgery and child pornography. And he provided expert testimony on behalf of the Department of Justice during the legal arguments surrounding the Communications Decency Act, which has just been overturned.

He said that while the laws gradually catch up with the science of computer forensics, investigations are conducted with the utmost care so that everything is above board. "We take a conservative approach. We make sure that we are over cautious. We use normal accepted forensic procedures but we double check everything. That way you can be confident if you are challenged in court."

Mr Schmidt sees the risks posed by computer literate criminals growing even further, especially as the popularity of the Internet continues to soar, and says authorities should be armed with the equipment and knowledge to tackle the problem.

"Computer crime investigation will become more and more important as even greater use is made of the technology in society," he said. "Law enforcement groups across the world have to recognise this and respond and react accordingly." ■

A Question of Privilege

A recent investigation in the UK has highlighted the difficult question of legal privilege where computer information is concerned. Here Jim Bates looks at the issues involved and what the implications are for computer crime investigators.

Legal privilege is a concept in British law which prevents certain types of information from being used as evidence in civil or criminal proceedings. For example, if a solicitor's records are being investigated in connection with alleged criminal activities, the police are only allowed to examine records directly connected with the investigation and cannot simply trawl through all of the records looking for information of specific relevance to the case. Quite apart from the fairly obvious problem that client confidentiality may be compromised, it should be noted that even unrelated information has potential value as intelligence. Thus even a brief glimpse of information which has no relevance to the current investigation may be remembered and used to direct the progress of a completely different inquiry.

The problems of determining how, where and when the principles of legal privilege should be applied are complex and difficult, and can only be decided by people with suitable legal knowledge and experience. However, consider a hypothetical investigation which legitimately requires examination of a solicitor's files.

This may result in an impasse since the investigator cannot determine whether information is subject to privilege without examining it, and if it IS privileged, the process of examination will have breached that privilege.

Quite clearly it is not satisfactory to accept the solicitor's evaluation of what is or is not privileged before material is examined because this is not an independent opinion. Neither can the question be decided by the investigator because he too is not an independent party to the investigation. Fortunately, the nature of computer based information and the accepted methods by which such information is investigated provide a relatively simple way out of this impasse. The example taken from investigation mentioned above will serve to illustrate the point.

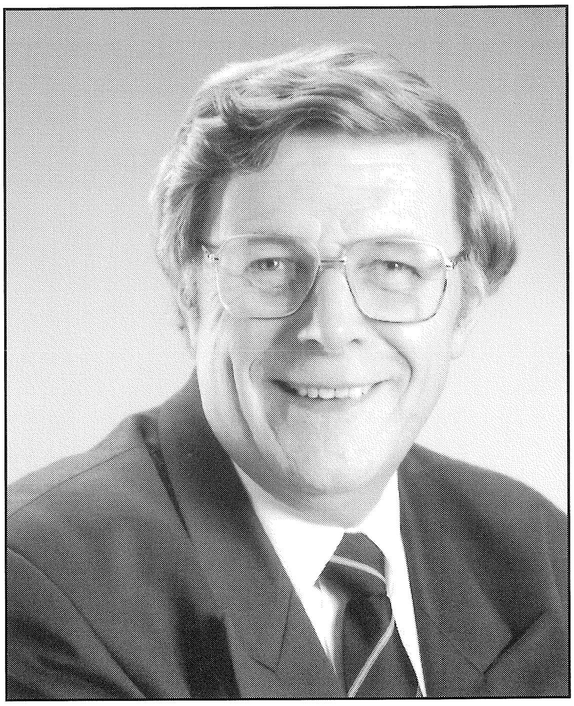
A civil order was issued to search an accountant's offices in connection with alleged accounting irregularities and naturally the investigators were anxious to examine computer records. The accountant and his legal representative attempted to prevent the computers from being copied on the grounds that a major proportion of the accountant's files were covered by legal privilege. After considerable (and sometimes quite heated) discussion between the opposing legal representatives and an adjudicating solicitor, the computer expert employed by the investigating team suggested a solution.

The copying process which would be used to collect the information from the computers was a forensically sound program which made no change to the original machine. While the copy was in progress, the only information revealed would be the total capacity of the disk being copied and the length of time that the copy was expected to take. No data content would be displayed and it would not even be possible to determine how much of the disk capacity was active data. Such information could not conceivably breach legal privilege and all of the information could thereby be secured. The copy process could be observed by any interested personnel to ensure fairness and once it was completed the copy could be sealed and placed in secure storage.

The accountant's machine could then be returned to normal use and the sealed copy would be taken to a suitably qualified, independent person who was acceptable to both parties. The process of determining the privilege status of the information could then be undertaken under strictly controlled conditions. The investigators would be satisfied that all of the information had been secured, while the defence team would be happy that an accurate determination of legal privilege could be made without the information being seen by the investigators. This solution was immediately accepted and the impasse was resolved.

The importance of this solution lies in the practical way that it satisfies the requirements of all the involved parties and allows the question of privilege to be placed squarely where it belongs - in the hands of the independent legal experts. The information could remain secured in such a manner that a need for subsequent access could be met if, for example, further investigation indicated that there should be a change in the parameters by which legal privilege has been determined. ■

Jim Bates is President of the Institution of Analysts and Programmers in the UK and has worked on numerous computer investigations.



Encryption

Dr Dorothy Denning is professor of Computer Science at Georgetown University in the US and her research is mainly in information warfare and information security, in particular cryptography technology and policy.

She has been studying the impact of encryption and other technologies on crime and her earlier work focused on intrusion detection, database security, cryptography, multilevel security and computer hackers. *She can be e-mailed at denning@cs.georgetown.edu.*

Together with William Baugh, vice president of the Science Applications International Corporation, she wrote a paper entitled 'Encryption And Evolving Technologies As Tools Of Organised Crime And Terrorism', delivered in May.

Here she summarises the paper to introduce the subject and give an overview of the implications it has for the fight against computer crime as well as warning investigators and police forces to take the threat seriously.

We are at the leading edge of what could become a serious threat to law enforcement and national security: the proliferation and use of robust digital encryption technologies. These technologies will be unbreakable, easy to use, and integrated into desktop applications and network services, including protocols for electronic mail, web transactions, and telephony. This paper discusses their impact on organized crime and terrorism.

We begin by summarizing actual cases where encryption was encountered, the scope of the problem, and the methods used by law enforcement to deal with it. Our findings suggest that the total number of criminal cases involving encryption worldwide is at least 500, with an annual growth rate of 50-100%.

We then discuss the threat posed by encryption to law enforcement, public safety, and national security. The threat is manifest in four ways: failure to get evidence needed for convictions, failure to get intelligence vital to criminal investigations, failure to avert catastrophic or harmful attacks, and failure to get foreign intelligence vital to national security. Encryption can also delay investigations, increase their costs, and necessitate the use of investigative methods which are more dangerous or invasive of privacy. Most of the investigators we talked with did not find that encryption was obstructing a large number of investigations. They were, however, concerned about the future.

Trends in the encryption market which impact law enforcement are reviewed next. One trend is the increasing integration of extremely strong encryption into commercial desktop applications and networks. The encryption will be easy to use and totally unbreakable. The worst case effect could be to render most communications and stored data immune from lawful access. Another trend, which has a balancing effect, is a growing market for key recovery systems that protect the owners of encrypted data from lost keys. These systems can give law enforcement agencies an alternative method of getting the keys needed to decrypt evidence.

Encryption is not the only technology which adversely affects law enforcement. There are other tools besides encryption, including cloned cell phones and steganography, that can be used to evade the police, conduct surveillance, or intrude into computers and networks. Many of these tools are enhanced by encryption.

Finally, we discuss encryption policy options, including export controls and domestic regulations in the United States and elsewhere, and their impact on crime and law enforcement. We review the Clinton Administration's encryption program to promote key recovery technologies through liberalized export controls, key recovery standards, and a voluntary licensing regime for key recovery agents.

In focusing on the seamy side of encryption and other technologies, we do not mean to imply that they are inherently bad or that their use should be restricted. Encryption in particular can be critical for safeguarding sensitive information. Business needs access to strong encryption to protect against espionage by competitors and foreign governments. Law enforcement needs encryption to safeguard sensitive communications relating to investigations. Individuals need it to protect their private communications and records.

Encryption policy must facilitate the sale, export, and use of strong encryption for legitimate purposes.

Not all cryptographic technologies pose a threat to society. It depends on whether the cryptography is used for confidentiality or authentication. The societal threat arises primarily with confidentiality services - what we refer to as encryption. Authentication technologies enhance investigations by ensuring the integrity and authenticity of evidence and its source. They are at least as important to electronic commerce and information security as encryption, perhaps even more so. Most computer intrusions result either from inadequate authentication or from design and configuration flaws that are not addressed by any form of cryptography.

Our central claim is that the impact of encryption on crime and terrorism is at its early stages. It is critical that we watch the situation closely and respond intelligently. Encryption policy must effectively satisfy a range of interests: information security, public safety, law and order, national security, the economic competitiveness of industry in a global market, technology leadership, and civil liberties. Meeting all of these interests is enormously challenging, but it is crucial that we find ways of protecting both freedom and order.

The full version of this paper is published by the National Strategy Information Center's Working Group on Organized Crime in the US. The WGOC, founded in 1996, brings together governmental and non-governmental specialists to improve analysis and operations against organized crime. ■

Book Reviews

Computer Law -

Third Edition. Edited by Chris Reed

Blackstone Press Ltd, London W12 8AW, UK
396pp ISBN 1-85431-448-3
£19.95

Computers are constantly in a state of flux, with technology making them ever more powerful, faster and capable. Consequently, the laws and regulations surrounding their use and misuse have to be flexible and readily adaptable.

The third edition of Computer Law is aimed at addressing all the latest legislation, as well as giving a comprehensive overview of the legal situation governing computer investigation and the prosecution of offenders.

While the second edition was only published three years ago, much has changed in the computer law field in that time. As the book's editor Chris Reed points out, three years ago very few lawyers had even heard of the Internet, and today many countries are attempting to sort what laws if any can be used or introduced to govern the Net's content and access.

Reed himself is Reader of Information Technology Law at Queen Mary and Westfield College, at the University of London. He has published many books on computer and telecommunications law and is a co-chairman of the Society for Computers and Law. The specialist authors in the book include solicitors, a barrister, senior lecturers and experts from the world of business.

The work gives an excellent introduction into the current international situation, with both academic and practical content that will be indispensable for anyone working in this field, be they lawyer or computer crime investigator.

Material covered includes copyright, patent protection, information security and data protection. Of particular interest to the investigator are chapters on computer crime and computer evidence used in court and electronic data exchange. These cover areas such as the Computer Misuse Act, classification of crimes, admissibility, privileged material, discovery and the authentication of material.

Also of interest are the chapters on hardware and software contracts and the issue of liability, which although intended mainly for manufacturers and distributors, is also relevant to anyone buying or handling computer programs.

A chapter on European Community law and its relevance to computers gives an insight into the trade changes as well as the restrictions and sanctions that are in place.

One of the main plusses of this book is the comprehensive listings of real-life cases and full tables of statutes, international legislation statutory instruments and EC secondary legislation. All are fully indexed and easily searchable.

While most of the cases and examples are focused on the UK, the work is firmly placed in the international context and is relevant to any investigator in the world.

The book attempts to cover a vast area by looking at almost every way in which the law affects computer users, and as such it succeeds admirably. However, its scope also means it cannot provide the sort of absolute detail that some may require, and even more specialist publications are available for that.

Having said that, Computer Law is highly recommended for anyone working with computers, and provides an excellent overview.

Digital Crime -

Policing the Cybernation

By Neil Barrett

Kogan Page, London N1 9JN, UK
224pp ISBN 0-7494-2097-9 £18.99

Neil Barrett earned fame and infamy as a computer hacker and by 1985 he was the UK's youngest computer science lecturer. Now, as one of the so called poachers turned gamekeeper, he works as a security specialist for Bull Information Systems and this is his second book after the State of the Cybernation.

Digital Crime provides an informative insight into the sheer scope and number of illegal computer activities that can and do go on. It is written in an easy to read and entertaining style, with topics including those on hacking, money laundering, viruses, the Internet and computer pornography.

Chapters on digital crime and the law and prosecution of offenders are interesting from the casual reader's point of view and give an idea as to the current powers police forces have as well as the problems both they and the courts face in the legal process.

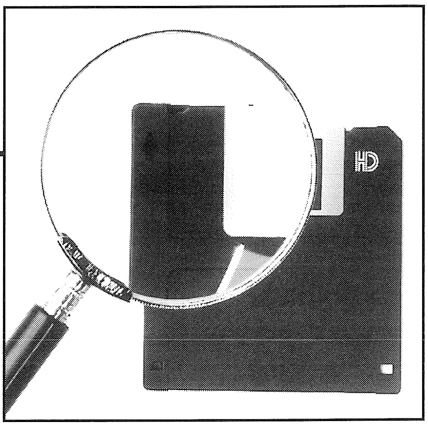
And Barrett also argues that police forces need to be up to speed on computers not only to catch computer criminals but also to speed up normal detective work. He cites the case of Peter Sutcliffe, the Yorkshire Ripper, as an example and says the murderer could have been caught much sooner had officers had a computer aided crime analysis system rather than wade through thousands of paper files.

A chapter on digital conflict takes the idea of crime one step further and Barrett says the world of linked computers means terrorists or other countries can wreak havoc on governments, the military and businesses. He likens the Internet to a Pandora's Box, a liberating technology that can threaten national, corporate and personal security.

But he says the key to preventing and investigating the darker uses of computers is knowledge and the willingness to confront the problem. As he says "Policing the cybernation is a task that the authorities have only recently begun to recognise. Jurisdiction, responsibility and the application of technology to combat technological abuse all need careful consideration - a process that has begun to gather momentum."

Overall the book is a good introduction into technology crime and for most people would be an insight into the potential that computers give criminals. Anyone entering this field for the first time will find it a good and interesting read, although the expert computer investigator or lawyer will probably be aware of most of the current issues. ■

Forensic Q&A



Q *To examine the contents of suspect computers I firstly make a copy of all the information onto a hard disk on a laptop. I then use this primary copy to write CD ROMS which I use for all subsequent analysis. Is this evidentially acceptable?*

A This may appear to be satisfactory at a superficial level but a deeper examination reveals serious flaws. The problem with this method, when used for evidential purposes, is that a new hard disk will need to be used each time a computer is copied. There are two major reasons for this.

The first copy made to the hard disk will be the primary copy and this must be maintained for use in court in the event of a legal challenge. If this copy is destroyed by re-using the hard disk on a subsequent investigation it will be impossible to prove in court that it was exact and error free. This is especially important when considering the drawback of the second stage of the process - writing to CD ROM - which has an inherent high error rate. Without the primary copy it will not be possible to prove that this has been done with 100% accuracy.

If a hard disk is re-used it will be necessary to prove that it does not contain any information remaining from a previous investigation. Since each primary copy is destroyed by re-use of the disk, dedicated programs and procedures will be required to ensure that cleaning of the disk is faultless, provable and exempt from human error. Even if such programs and procedures existed, a further complication is that there is no legal precedent for the use of this method, which would have to be proven and accepted in court.

The economic and practical implications of the above (i.e. the need for a constant supply of new hard disks and the long term storage of primary evidence hard disks), together with the serious legal issues raised by any potential solutions, suggest that the method is inadvisable for use for evidential purposes.

Q *When DOS allocates space on the hard drive does it look for the next sequentially available cluster from the beginning of the disk?*

A This is a much more complex question than it appears. The short answer is no because if DOS always did this, the end portion of the available disk space would only be used when the disk became full and the earlier portions would get far more than their fair share of use.

On the other hand, if DOS relied upon a constantly cycling pointer to ensure even use across the disk, applications might become slow as they needed to access data in widely separated areas of the disk.

As far as I am aware, there are three ways that DOS attempts to prevent this happening: firstly, as long as the machine is switched on, a pointer is maintained to indicate the next cluster earmarked for use and this is where the search for space will begin. Secondly, the amount of space required by the calling application determines which space is actually allocated. Thirdly DOS will always attempt to maintain continuity of data files by attempting to allocate space as close to the end of a current file as possible.

Q *Analysis of the physical location of files on the hard disk frequently, but not always, shows the Windows swap file in a physically separate group of clusters to the rest of the data. Why is this and what controls the location of the file - Windows or DOS?*

A Windows was designed to work within a widely variable memory space. This presented problems of compatibility since Microsoft were not happy to have their new operating environment falling over because the user did not have sufficient memory. So the concept of swap space was introduced.

This allowed the software to treat the disk space as an inactive extension of the RAM whereby currently inactive programs and data could be written temporarily to the disk while their RAM space was used by another application (using a temporary swap file).

Unfortunately, the old style DOS allocation system is notoriously slow and swapping RAM to disk in this way caused serious degradation in system performance. The swapping concept was therefore improved by pre-allocating a dedicated area of the disk in a single contiguous chunk as a permanent swap file.

Windows knows precisely the size and location of this file and can read and write information to it using a more efficient management system than DOS. The temporary swap file is created and destroyed by DOS as requested by Windows, while the permanent swap file is created once by DOS during Windows configuration and used thereafter directly by Windows. ■

If you have any tips, advice or cautionary tales you would like to share with readers, please contact the Journal.
e-mail your questions and comments to ijfc@pavilion.co.uk

Although every effort is made to ensure the accuracy of these answers, they are presented for general information and may not apply in rare specific cases. Readers are advised to seek confirmation from an independent specialist in forensic computing when dealing with evidentially valuable material.

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

InfoWarCon '97

10-12 September, Sheraton Premiere, Tysons Corner, Virginia, US.

Solutions oriented conference, addressing infosecurity and infowar-defense needs of the military, law enforcement (US and international), private sector and commercial infrastructure. More than one hundred senior representatives from over thirty countries will have the opportunity to interact at InfoWarCon '97. International presenters will examine the legal, commercial and technical problems envisaged with the merging of information warfare and information security. Pre-conference tutorials include Malicious Software: Detection and Eradication.

Contact: National Computer Security Association
Tel: +1 717 241 3233
Fax: +1 717 243 8642

The 2nd International Telecommunications Fraud and Crime Conference '97

15-17 September, London School of Economics

Exclusively for Law Enforcement and Telecommunications Industry Professionals The 1997 FCS Conference will be addressing the worldwide problems of international crime and fraud in the communications industry. The industry is becoming more complex and more sophisticated; the opportunities for fraud even greater. This year's event brings international guest speakers from law enforcement agencies and experts within the telecommunications industry looking at new technologies, new frauds and the results of successful industry and police co-operation. Prior to the two day conference there is an interactive workshop designed for all delegates to obtain full value from the main conference by appreciating the technical background, trends and potential telecommunications crime affecting fixed line, cellular, paging and satellite operations.

Contact: David Harrison, conference organiser
Tel: +44 (0)181 289 9595
Fax: +44 (0)181 289 9696

The International Information Security Managers Symposium

16-18 September, London

The symposium is designed around the informational exchange of roundtable discussions and informal presentations. In a relaxed atmosphere, led by experts and industry leaders, delegates will trade experiences, strategies, and techniques with those who share their concerns and problems.

Contact: MIS Training Institute
Tel: +44(0)171 779 8944
Fax: +44(0)171 779 8293

ICCE 97 - International Customs Conference and Exhibition

16-18 September, Brighton, UK

High level conference and major trade exhibition. It will be attended by delegates with a broad range of responsibilities from HM Government, senior members of international governments and agencies. The event will discuss issues surrounding the operational management, reform and modernisation of Customs & Excise services throughout the world.

Contact: M4 Marketing Communications Ltd
Tel: +44(0)1635 40676
Fax: +44(0)1635 43275

Financial Fraud in South America

25-26 September, Miami
Contact: D&D Comunication, Milan
Tel: +39 2 58 30 61 65
Fax: +39 2 58 31 56 55

COPEX UK

30 September-2 October, Farnborough, UK

Contingency and operational procurement exhibition

Contact: Tracey Dunn, Copex
Tel: +44(0)1923 819301
Fax: +44(0)1923 818924

Money Laundering in Spain and South America

23-24 October, Madrid
Contact: D&D Comunication, Milan
Tel: +39 2 58 30 61 65
Fax: +39 2 58 31 56 55

International Conference on Forensic Computing

3-5 December, The Grand Hotel, Brighton, UK

A unique three day conference to be addressed by speakers from across the world, covering computer crime, investigation and forensic evidence. Experts from a wide range of forensic computing fields will be attending, as well as exhibitors from firms involved in this fascinating area.

Contact: International Journal of Forensic Computing
Tel: +44(0)1903 209226
Fax: +44(0)1903 233545
e-mail: ijfc@pavilion.co.uk

TRAINING

Training in Computer Forensics

Four modules comprising:
Fundamental Computer Forensics
Applied Computer Forensics
Advanced Computer Forensics
Legal and Procedural Computer Forensics
Courses held monthly in West Sussex.

Contact: Computer Forensics Ltd
Tel: +44(0)1903 823181
Fax: +44(0)1903 233545

PEOPLE

Computer expert **Jolyon Ralph**, known for his forensic work with Amigas, has joined Top Hat Computing based in Croydon as a senior consultant. Jolyon will continue to offer his forensic services in the Amiga field, and also in investigating Windows 95/NT systems and the Internet. He can be contacted by telephone on *+44 (0)181 680 4860* or e-mail on *jralph@cix.co.uk*

Nick FitzGerald is the new editor of the Virus Bulletin, the publication which examines computer viruses and their detection and removal, and can be contacted by e-mail on *nick@virusbtn.com*

International Journal of
FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd.