
We Trip The Light
FANTASTIC

Computer Law & Security Report (2005) 21, 357–358

ELSEVIER

Computer Law
&
Security Report

EDITORIAL

Definitive digital maps pose a challenge for e-Government

For some time now the Government has been extolling the virtues of the digital environment. This has extended in all kinds of ways into policy development and been given the label e-Government. In 2004 the e-Government Unit was established, based in the Cabinet Office, to work with departments ''to deliver efficiency savings while improving the delivery of public services by joining up electronic government services around the needs of customers''. Much of what this is about concerns public procurement in providing technology that will enhance the experience of customers when interacting with Government. The Head of the Unit, Ian Whatmore, is to be a 'thought leader' and 'catalyst for change' in the adoption and management of technology in Government and to develop best practices in technology adoption across Government.

One of the challenges here is to actually translate these aspirations into better products and services. One area, in particular, concerns the potential of using digital maps to define the legal boundaries of common land, public rights of way and national parks etc. Ordnance Survey which operates as a Government agency, with substantial control of its budget and spending has, in recent years, developed *OS MasterMap* — an intelligent digital map designed for use with geographical information systems (GIS) and databases. Building upon this, in 2001, the OS announced the launch of the 'digital national framework' as a model for the integration of geographic information of all kinds. As such this will assist a wide range of businesses and organisations seeking a referencing system to link business with geographic information.

This is to be welcomed but what has not happened yet is the linking of definitive information about the location of public rights of way, common land etc. into digital map format. This is a big issue for landowners, farmers, environmentalists, planners and policy makers who want to reap the benefits that technology can offer in terms of access, accuracy and cohesiveness of the dataset that an online version could offer. Currently, the paper based versions of such mapping data are inadequate, incomplete and out-of-date — a fact brought home to Government in 2001 during the outbreak of 'foot-and-mouth' disease in cattle when no up-to-date online national grid of public rights of way existed to assist the authorities to manage public access to the areas badly affected by the disease.

Currently, the Commons Bill (HL), which updates the law on the registration of common land and town or village greens is proceeding through its Parliamentary stages. It provides for commons registration authorities to continue to keep registers and for the appropriate national authority to establish commons associations with powers to protect and promote sustainable agriculture on common land etc. Clause 24 of the Bill enables the appropriate national authority to make regulations permitting or requiring commons registration authorities to maintain commons registers in an electronic form. Converting evidential data as to exact boundaries of different types of land presents complex challenges, as the digital copy must stand up to scrutiny in a court of law. It is precisely this type of issue that e-Government policies must address if the long-term strategy of building on the digital revolution is to be realised

0267-3649/$ - see front matter
doi:10.1016/j.clsr.2005.08.011

within Government. The explanatory note to the Bill puts the position succinctly:

''The digitisation of the register maps of common land undertaken by the Countryside Agency and the Countryside Council for Wales for the purposes of the statutory right of access under Part I of the Countryside and Rights of Way Act 2000 has highlighted the difficulty of translating the information contained in old, relatively small scale Ordnance Survey register maps held by commons registration authorities into a modern electronic mapping database, and particularly in determining and locating accurate boundaries to registered land where the register maps are poorly drawn, indistinct or based on out-of-date mapping.''

More work need to be done to co-ordinate this task. It is going to involve a long-term consolidation of the definitive map and a resolution of the backlog of disputes and appeals that have built up over time. Up to now the only broad based provision supporting the e-Government agenda in this respect have been Sections 8—9 of the Electronic Communications Act 2000 (Ch.c.7). These sections enable the appropriate minister to issue regulations to authorise or facilitate the use of electronic communications or electronic storage, where previously other forms of communication or storage were required to satisfy evidential requirements.

It is going to take some time to resolve these challenges but, in the long term, it is only by tackling such problems that the real breakthrough can be achieved in fully embracing the potential of the digital revolution.

Stephen Saxby
E-mail address: s.j.saxby@soton.ac.uk

New Report Correspondents

Roger Clarke

Roger Clarke is joining the Panel in order to augment CLSR's technical and executive perspectives. Roger is based in Canberra, Australia. His consultancy work focuses on strategic and policy aspects of e-Business, information infrastructure, and data surveillance and privacy. He has been associated with universities throughout his 35-year career in the information technology industry. Most relevantly, he is a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W. in Sydney. He is also a Visiting Professor at the Australian National University, and the University of Hong Kong. In the e-Business area, he will apply his expertise in technology evaluation, architecture, trust, security, e-consent, privacy, authentication, digital signatures, public key infrastructure and biometrics. He has long experience in privacy impact assessments, particularly in government contexts. He has a specific interest in e-Publishing, including discovery strategies and metadata, but importantly also copyright, digital rights management, information management, and information policy. Because of his academic and government involvements, he has paid particular attention to open source, open content, and the open access/e-Prints movements. He also works in Internet architecture and governance, 'growing pains' (such as spam, cookies, censorship, malware, evidence of identity and location, domain-names, P2P and digital property rights), cyberculture, collaboration technologies, and the history of the Internet. He has provided expert evidence in a variety of patent cases (regarding smart cards and Internet commerce), and in relation to defamation on the web (including for **Dow Jones v. Gutnick**), domain-names, privacy, and P2P technology.

David Taylor has joined the correspondents' panel. David holds a Masters in Engineering and PhD in Physics. Having retrained as a solicitor, David now works in the Lovells Intellectual Property, Technology and Media practice in Paris, advising on many aspects of e-commerce and intellectual property rights on the Internet, including domain names, for which Lovells offers Anchovy, a global online brand management and protection service. David is a member of the WIPO Arbitration and Mediation Centre's Domain Name Administrative Panel and is a panelist for .fr with CMAP (Centre de Médiation et d'Arbitrage de Paris).

Computer Law & Security Report (2005) 21, 359–377

Computer Law
&
Security Report

CLSR BRIEFING

News and comment on recent developments from around the world

Compiled by Stephen Saxby, editor

United Kingdom

LSE identity card report published

The London School of Economics, in partnership with Enterprise Privacy Group (EPG) an information consultancy, has published a report on the Identity Cards Bill. This follows a six months' wide ranging research project intended to examine a number of issues raised by the Government when it first proposed its national identity system. The report concludes that the establishment of a secure ID card scheme will have the potential to create significant though limited benefits for society. It notes, however, that the proposals currently being considered by Parliament are neither safe nor appropriate. Stakeholders involved in the report indicated that the proposals were ''too complex, technically unsafe, overly prescriptive and lacking a foundation of public trust and confidence''. The report, therefore, considers alternative models for an identity card scheme that the research indicates may achieve the goals of the legislation more effectively. The report notes that many of the public interest objectives of the Bill might be more effectively achieved by other means. For example, it suggests that preventing identity theft may be better addressed by giving individuals more control over the disclosure of their own personal information, while the prevention of terrorism ''may be more effectively managed through strengthened boarder controls and increased presence of borders, while allocating adequate resources for conventional police intelligence work''.

The report also criticises the technology envisioned for the scheme which it suggests is largely untested and unreliable. It notes that no scheme on this scale has been undertaken anywhere else in the world but smaller and less ambitious systems have encountered substantial technological and operational problems. The use of biometrics gives rise to particular concern because this technology has never been used on such a scale.

The report also indicates that the likely cost of a ten year role out of the proposed scheme will be between £10.6 billion and £19.2 billion with a median of £14.5 billion. This figure does not include public or private sector integration costs and takes no account of any potential cost overruns.

The report suggests that any system that supports critical security functions must be robust and resilient to malicious attacks. With the size and complexity of this system security measures are likely to result in substantially higher implementation and operational costs than originally estimated. It notes that the proposed use of the system for a variety of purposes and access to it from a large number of private and public sector organisations will require unprecedented attention to security.

The report concludes that the success of a national identity system will depend on ''a sensitive, cautious and co-operative approach involving all key stakeholder groups including an independent and rolling risk assessment and a regular review of management practices''. The researchers state that they are not confident that these conditions

0267-3649/$ - see front matter
doi:10.1016/j.clsr.2005.08.010

have been satisfied in the development of the present Bill. It concludes on a serious note that the risk of failure in the current proposals is ''magnified to the point where the scheme should be regarded as a potential danger to the public interest and to the legal rights of individuals''.

Editor's note

The London School of Economics Report is available at http://is.lse.ac.uk/idcard/

Public sector ICT abuse still a major risk

ICT fraud and abuse are still posing major problems to public sector organisations and those who use their services, an in-depth survey shows.

New technologies, like the use of handheld devices (PDAs) and wireless networking, are creating fresh risks that public services are only slowly reacting to. And, despite better ICT security systems, a 'culture of complacency' and a failure to ensure that staff understand the rules is undermining the effectiveness of ICT security arrangements.

The survey, carried out in 2004 by the Audit Commission, is based on the responses of more than 400 public sector organisations, including NHS trusts, local authorities, police and fire authorities. Two hundred cases of ICT fraud and abuse were identified in the survey. The results are published in the report *An Update on ICT Fraud and Abuse 2004*.

Since the last survey in 2001, the new report points to some improvement in ICT security, with security policies in place at 96% of organisations. It also records a fall in the incidence of 'business disruption' (viruses or other deliberate acts aimed at denying users access to systems), making up only 20% of cases in the 2004 survey compared with 39% in 2001. But the report does reveal:

- a 13% growth in reputational risks, including staff accessing pornography or other inappropriate material (52% of cases in 2004 compared to 39% in 2001);
- financial risks continuing to mount (28% of cases in 2004 compared to 22% in 2001); and
- evolving technology (like wireless networking) presenting a challenge that organisations do not fully appreciate (64% of respondents put wireless networking in the low/medium risk category).

The report focuses on the key role staff play in ICT security. Yet only 50% of organisations initiate staff training in ICT security systems, and only a third of organisations inform their staff about their ICT security policy and what staff should be doing.

Alongside the report the Commission has produced a self-assessment questionnaire for chief executives and other senior managers to use when considering their own organisation's susceptibility to ICT fraud and abuse.

Steve Bundred, Chief Executive of the Audit Commission said:

''The growth in new technology — through PDAs and wireless networking, for example — coupled with the greater sophistication of hackers and fraudsters mean that the risks remain significant. ICT security is only as effective as the staff within the organisation, and too often we are finding that staff are unsure of their role. If we fail to get this right we risk eroding the confidence of citizens in the electronic systems that underpin public services. We recommend that chief executives and other senior staff review their organisations against the set of questions we've developed.''

To help local government and health bodies tackle ICT fraud and abuse, the Commission has developed the *Your Business at Risk* (YBAR) database, against which organisations can compare their ICT security measures against a range of other organisations. To use YBAR, local government and health bodies should contact their appointed auditor.

Editor's note

The seventh ICT fraud and abuse survey was carried out during October—November 2004. Four hundred and seven bodies completed the survey, including local government, police and fire authorities, NHS bodies, central government departments, non-departmental public bodies and agencies.

See further: www.audit-commission.gov.uk

Public needs should drive digital innovation

Transforming society through technology is in danger of happening too quickly and leaving the public behind, according to the Institute for Public Policy Research (IPPR) which today published a manifesto for a digital Britain. It concludes that government has prepared the UK well for the 21st century but remains seduced by vague notions of a ''knowledge economy'' and is too often driven by innovation for its own sake.

The report argues for directing technological advance to meet social and economic benefits and

ensuring that legal and constitutional priorities — including privacy and democratic participation — are not undermined. It concludes that people are more likely to embrace technology if they have more choice about how and when it is used to store information and access services.

Modernising with Purpose: A Manifesto for Digital Britain recommends:

- *Privacy Impact Assessments*: all government departments should perform a Privacy Impact Assessment when developing new legislation to help service providers decide when to share data. This could be modelled on the generic Privacy Impact Assessment being developed by the Department for Constitutional Affairs (DCA).
- *Targeted ICT training*: the Government should investigate how Sure Start can be used to improve the IT skills and media literacy of parents. Initiatives like giving access to medical records online risk failure if parents do not have the right skills to access them.
- *New e-government targets*: these would be based more explicitly around user satisfaction and include calculations of time savings and service quality.

William Davies, IPPR Senior Research Fellow and report author said:

''Government has done well on issues like rolling out broadband and getting computers into schools. However, there is a danger that in the name of modernisation, policy is informed by a blind faith in technology and an imagined digital future rather than a clear sense of purpose. People need to believe that technology is something we can harness rather than something that just happens to them. Innovation has to be lead by the needs of the public, rather than vice versa. This is as much a challenge for industry as it is for Government.''

Editor's note

Modernising with Purpose: A Manifesto for Digital Britain by Will Davies is available to buy from www.ippr.org

Consultation on UK implementation of the IP Enforcement Directive

The Patent Office has launched a consultation setting out proposals for implementing the Directive on the enforcement of intellectual property rights 2004/48/EC which was adopted in April 2004. Member States are required to implement the Directive by 29 April 2006.

The Commission submitted their original proposal for a Directive to ensure the enforcement of intellectual property rights in March 2003. The European Parliament's Committee on Legal Affairs and the Internal Market agreed their report on the Directive in November 2003, and informed the Council of Ministers that they hoped the Directive could be adopted at First Reading. Following the European Parliament's report, there were intensive negotiations in the Council Working Party and Permanent Representatives Committee which resulted in a compromise proposal that was adopted after a First Reading in April 2004. Significant changes were made in the adopted Directive compared to the Commission's original proposal.

The Directive is broadly consistent with the current UK framework for the enforcement of intellectual property rights and provides a basis for harmonising civil measures available to enforce intellectual property rights across the European Community. The Commission's original proposal included criminal sanctions, but most Member States (including the UK) considered it inappropriate to include them in such a Single Market measure intended to encourage the free movement of goods.

IP crime has a serious economic effect in the UK and across the European Community, and the Patent Office is continuing to adapt its role in helping fight intellectual property crime. Its *IP Crime Group* published the first *National IP Crime Strategy* in August 2004 and the first *National Enforcement Report* was produced in 2005. The Commission's current work programme also includes two new proposals for criminal sanctions for intellectual property infringements, which it expects to finalise shortly.

The consultation includes a *Partial Regulatory Impact Assessment* that concludes that the implementation proposals strike the right balance between effective enforcement of intellectual property rights and over-regulation. The Patent Office believes this is particularly important bearing in mind the *Better Regulation Action Plan* announced by the Chancellor of the Exchequer (Gordon Brown) last May.

Editor's note

The consultation on EC Directive 2004/48/EC will run until 7 October 2005. Further information from: www.patent.gov.uk/about/consultation/enforce05/indec.htm

Ofcom publishes annual report for 2004–2005

Ofcom has published its Annual Report and Accounts for the period 1 April 2004 to 31 March 2005.

In 2004/2005 Ofcom sought to deliver against four key priorities. These were:

- to put in place swift and effective solutions to remove unnecessary regulation, resolve market distortions, reduce prices and take action to protect consumers;
- to make significant progress in Ofcom's strategic reviews of the sector;
- to consolidate the post-merger efficiency gains of the prior year of establishment in order to improve effectiveness; and
- to do all of this with an operating budget 8% lower in real terms than the operating budget for 2003/2004.

The Report notes that unnecessary regulation imposes costs on business, stifles innovation and provides a barrier to market entry, increasing prices and diminishing choice for consumers as a consequence. Ofcom therefore would seek to be a deregulating regulator where feasible, operating under a bias against intervention and with a commitment to seek the least intrusive regulatory mechanisms to achieve specific policy objectives. The Report lists specific examples of targeted deregulation.

With regard to regulatory activity, during the period under review, Ofcom's four strategic reviews — in telecommunications, spectrum, public service broadcasting and radio — either reached their conclusion or passed important milestones.

Ofcom also took immediate steps to further market development and to protect the interests of citizens and consumers.

In telecommunications, Ofcom:

- took action to support lower prices and greater competition in broadband, including a 70% reduction in local loop unbundling wholesale rental costs;
- took action to protect consumers from abuse of sales and marketing techniques, such as misselling and slamming, in fixed-line telecoms;
- required a reduction in mobile phone network termination charges, leading to lower prices for consumers;
- took action in the premium rate services market to strengthen consumer protection and increase confidence in the governance of the industry.

In spectrum, Ofcom:

- took action to support progress towards digital switchover in television, including clarity on timing, the establishment of SwitchCo and incorporation of switchover obligations in commercial public service broadcaster licences.

In broadcasting, Ofcom:

- finalised the new Broadcasting Code, with simplified rules and greater protection for children and protection of freedom of expression for adults;
- completed research into the role of television advertising in the context of the wider public debate on childhood obesity and took action to strengthen rules governing television advertising of alcohol;
- agreed measures to ensure broadcasters meet statutory obligations to provide access services such as subtitling and audio description; and
- launched the UK's new third tier of radio — community radio — for local groups interested in not-for-profit broadcasting with a simple, low-cost licence.

Commenting Ofcom Chairman David Currie said: ''The communications sector underpins the UK's economic prosperity and our political democracy. Effective regulation plays a key role in ensuring those benefits flow to every consumer, business and community.''

Editor's note

Further information from www.ofcom.org.uk

Mobile content classification — will it make a difference?

At last we have a classification framework for mobile content! Published on 7 February by the newly formed Independent Mobile Classification Body (''IMCB''), the ''*Guide and Classification framework for UK Mobile Operator Commercial Content Services*'' is the first of its kind in the world. Whilst this is clearly a welcome development in the campaign to protect children from accessing unsuitable content via mobile phones will it make any difference in practice?

How will it affect Content Providers?
Under the framework Content Providers must self-classify visual content (i.e. still pictures, video and audio—visual content, including mobile games) to identify content which is suitable only for adults (18 years plus). They face a number of challenges in doing so.

As this framework is a world ''first'' they will have to decide where the boundaries lie in those difficult borderline cases without having a body of accepted industry practice to refer to. Although the IMCB is offering a non-binding advice service, it may charge for this. Hardly the incentive Content Providers need to take classification seriously.

The inherent ''subjectivity'' involved in classification makes the process harder. Although the framework lists certain types of content which must be 18 rated (i.e. content featuring strong and foul language; sex; nudity; violence; drugs; horror and imitable techniques), it acknowledges that an 18 classification may not be appropriate in all cases. Just because a piece of content contains violence doesn't necessarily mean it is unsuitable for children. One only has to consider the violent antics depicted in ''Tom and Jerry'' cartoons to appreciate that the context and way the material is presented are also relevant to the assessment.

Content Providers cannot ignore other regulations or codes of practice because they have self-classified their content. If the content is being delivered by a premium rate service mechanism they will also need to comply with the ICTIS Code on Premium Rate Services. Also, there is scope for Operators to require more detailed classification than the simple 18 plus benchmark in the framework.

Most significantly there are no formal sanctions for ''misclassifying'' content and it is left to the Operators to police this though their contracts with Content Providers. It is unclear how this will work in practice. What incentives will there be on Content Providers to take classification seriously? Shouldn't Operators also take some responsibility? After all they decide and control ultimately what is published on their decks?

What does it mean for parents?
From a parent's perspective one has to ask ''Does the framework go far enough''? It does not address the area of greatest risk; that of children accessing unsuitable content via Internet connections and WAP applications on their mobile devices. It only applies to content containing visuals or graphics. Text, audio and voice services only are outside its scope despite the fact they could contain equally unsuitable content. In addition there is nothing to stop your 10 year old downloading the most violent of mobile games whilst you are ''roaming'' on holiday abroad. The framework only applies to content which is to be provided to UK customers of UK mobile Operators.

How many parents have heard of the IMCB or know the classification framework exists? A classification guide can only be effective if it is actually used and the boundaries of what is and is not suitable tested and challenged. Parents need to be informed of the framework and their rights to complain to their Operator, the IMCB and ultimately its appeal body if they consider an item of content has been misclassified.

Conclusion
On its own the framework is unlikely to make a difference. Other measures are required if we are to find an effective solution to protect children from accessing unsuitable content via mobile devices. Yes, the framework is helpful. Yes, it will help focus the minds of those responsible for distributing content as to what should be restricted. However, if Content Providers are to take classification seriously they need incentives to do so. Also, we need effective technical solutions to ensure that when content has been classified as ''restricted'', access to it is ''in fact'' restricted. On this front we can learn from measures being taken elsewhere. Children in Belgium have been the first to be issued with new ''smart'' identity cards to protect them in the online environment and prevent paedophiles posing as children in online chat rooms. Perhaps this could be applied to the mobile Internet environment. Most importantly parents and children need to be informed of the classification scheme and educated about the responsible use of mobile devices.

Mathilde Heaton
Solicitor, DLA Piper Rudnick Gray Cary UK LLP

New division to tackle business over personal information

The Information Commissioner's Office has established a new division devoted to protecting personal information held by businesses. The new Regulatory Action Division will use the Commissioner's powers to regulate the behaviour of organisations and individuals that collect, use and keep personal information, to ensure compliance with the Data Protection Act 1998.

Assistant Commissioner (Regulatory Action) David Smith said:

''Changes in the structure of the Information Commissioner's Office that have come into effect this

week are designed to make life tougher for the minority of businesses that don't take their data protection obligations seriously. Previously complaints were handled by a compliance team, but now for the first time the ICO has teams of specialists devoted solely to using the Commissioner's powers to bring about compliance with the law. Negotiation will usually be our first option, but we won't hesitate to take legal action swiftly against businesses where the circumstances warrant it.''

There has been a recent 'explosion' in the number of businesses holding personal information, and with that surge, an increase in the potential for the information to be misused. The Regulatory Action Division will use powers, including criminal prosecution, non-criminal enforcement and audit to ensure that personal information is properly protected. It will take action wherever data protection obligations are ignored, examples need to be set or issues need to be clarified. This will include acting against organisations which are required to register with the Commissioner's Office, but fail to do so.

Editor's note

Forms of Regulatory Action available to the division include:

- ***Criminal prosecution**: available where there has been a criminal breach of the Data Protection Act (Section 61).*
- ***Caution**: an alternative to prosecution where a criminal offence has been admitted but a caution is a more appropriate response.*
- ***Enforcement notice**: a formal notice requiring an organisation or individual to take the action specified to bring about compliance with the Act.*
- ***Application for an enforcement order**: an order issued by a court requiring a person to cease its behaviour which is harming to consumers.*
- ***Audit**: the organisation assents to an assessment of its practices of processing personal data to ensure it follow good practice.*
- ***Negotiation**: will be used widely in order to bring about compliance with the Act and related laws.*

The Division is made up of four units:

- ***Remedies unit**: works towards the negotiated resolution of non-criminal cases.*
- ***Audit unit**: systematically checks a business' compliance.*
- ***Enforcement unit**: responsible for non-criminal enforcement action in cases where negotiated resolution is inappropriate or not possible.*
- ***Investigations unit**: brings professional investigatory skills, particularly in relation to criminal cases.*

Further information from: http://www.informationcommissioner.gov.uk/

Asylum Bill raises privacy dangers from passenger surveillance says the Law Society

Government Plans for the routine and comprehensive capture and retention of passenger and crew information for all air, sea and rail travellers into and out of the United Kingdom are disturbing according to the Law Society.

Proposals in the Immigration, Asylum and Nationality Bill debated before the summer recess in the House of Commons provide the legislative framework for the Government to award a contract for e-Borders technology. As well as allowing the authorities to routinely capture and share all passenger and crew information it would also give them the power to retain reservation and payment data to build up a picture of people's travel itineraries.

Clauses 23–36 of the Bill provide a legislative foundation for the Government's ''e-Borders'' programme. Routine and comprehensive data capture and sharing powers are proposed in respect of passengers, crew, service and freight arriving or leaving the United Kingdom. Passenger data will be retained and, along with reservation data, will be profiled. The Government acknowledges that much of the detail is to be decided in secondary legislation and that precise costs, and who will bear them, have not yet been settled. It anticipates that carrier check-in transaction times will be extended and has said that it is doing work to establish the practicality of charging passengers a fee to cover costs.

Janet Paraskeva, Law Society Chief Executive, is urging the Government to reveal more about its plans:

''The creation of passenger audit trails and the use of data profiling raise serious privacy issues. In light of complementary Government initiatives, like the proposed National Identity Register, we would echo concerns about the dangers of a move towards a surveillance society.''

The Government acknowledges much of the detail of its proposals will be left to secondary legislation that costs are uncertain and may fall on passengers and that check-in times will be

affected. The Law Society believes that the history of Government IT failures does not bode well for the practical implementation of an initiative that seeks to handle hundreds of millions of arrivals and departures to and from the UK. The Government should pause for thought, engage in a wider debate and, in future, subject such proposals to full and independent Privacy Impact Assessments.

Editor's note

The Law Society regulates and represents the solicitors' profession in England and Wales and has a public interest role in working for reform of the law.

Magistrates to access new database to track down missing offenders

Magistrates' courts across England and Wales are to gain electronic access to one of the country's largest databases to help track down missing offenders who ignore fines and other court penalties. The partnership between the Department for Constitutional Affairs and the Department for Work and Pensions means that courts' staff will be able to instantly check the latest whereabouts of missing offenders who have changed address without notifying the courts, by accessing the DWP's electronic Customer Information System (CIS).

Whilst the database contains extensive records on about 85 million people, including defaulters who have moved abroad or died, magistrates' courts will only be able to access basic personal details such as name, address, date of birth and national insurance number.

Constitutional Affairs Minister Rt. Hon. Harriet Harman QC MP said:

''One of the problems with fines enforcement is that it's difficult to get up-to-date information on where criminals are staying so it's hard for magistrates' courts to track them down quickly. But the courts will soon have access to a whole lot of information that they can't get any other way. This means they can catch up with offenders who have moved house and refuse to obey the court much more quickly and easily.''

National rollout of the database should be complete by mid September. It is anticipated that dedicated courts' staff will make up to 340,000 enquiries in total each year. Magistrates' courts have already been given access to a credit reference agency database to help track down offenders. Access to existing databases is part of a concerted effort to give courts the intelligence they need to track offenders' movements and make them comply. It is also regarded as cost effective.

Editor's note

Whilst magistrates' courts have previously been able to access the Department for Work and Pensions' (DWP) database to crack down on people who willfully ignore court orders, the manual process was inefficient and ineffective.

The Customer Information System (CIS) is also linked to Inland Revenue's databases and includes personal data records for those in employment, in receipt of Child Tax or Working Families Credit as well as state benefits and pensions.

Access to the credit reference agency Equifax database occurred on 5 November 2004. More than 95% of criminal cases begin and end in magistrates' courts.

Survey shows IT profession see risk of removable media but turn a blind eye!

According to a survey on ''*Removable Media in the Workplace*'' companies' information security expenditure could all be for nothing as they turn a blind eye to the threat of removable media. The research, conducted by mobile security specialists Pointsec, shows that removable media devices, such as media players and USB flash drives, are now routinely used by a huge number of employees in the vast majority of UK businesses, but with little regard to the security threat they pose. A surprising two-thirds of IT professionals who use USB flash drives themselves at work admitted that they did not protect them with encryption even though they are aware of the associated dangers.

The survey highlights that a large number of organisations are yet to address the problem of removable media. With removable media plummeting in price, memory capacity soaring and more people using them at work, companies need to be aware of how easy it is for staff to use them, lose them or take competitive information away on them, all in the palm of their hands. If lost or stolen, vast amounts of valuable company information could seriously expose a company to extortion, digital identity fraud, or damage to their reputation, integrity and brand.

Some of the headline statistics from the survey, conducted amongst 300 UK IT professionals

(many of whom are IT security managers), reveals that:

- removable media devices are being used in 84% of companies;
- on average 31% of employees within a company are utilising them in the office;
- 90% of those surveyed were aware of the potential danger that removable media presents;
- a third of organisations state that removable media is being used within their company without authorization;
- 41% of IT professionals are not aware how easy it is to protect the data on a removable media device.

Martin Allen, Managing Director of Pointsec UK said:

''There seems little point in companies spending vast sums of money on information security if at the same time they're letting their staff use these devices at work which allow them unhindered access to download vast quantities of sensitive company information. Storing information on devices is not a new problem — not so long ago it would have been information stored onto a 1.5 mb floppy disk, however, now the problem is a much greater storage problem and therefore, needs to be dealt with in the security policy. Organisations need to introduce strict guidelines on the use of removable media devices in the workplace, as well as investing in encryption software which will allow administrators to force the encryption of all data put onto a mobile device. Using this type of software is just as vital and inexpensive as using anti-virus software, yet only a fraction of organisations have woken up to the problem.''

The proliferation of high capacity media players and USB flash drives on the market makes it possible to save anything up to 100 GB's of information on one. This means an employee could download four million documents of valuable data on what appears at first sight to be just an entertainment tool. USB pen drives and USB memory sticks can now store 4 GB's of memory which equates to around 160,000 documents.

In addition, employees could unintentionally expose their organisation to infection from viruses, worms or other types of malware when these devices are used to transfer data from non-company controlled computers to the user's computer at work.

To secure your company from the security implications associated with removable media and mobile devices Pointsec recommend that you:

- deploy user mobile guidelines or ensure that your corporate IT security policy includes corporate directives that state the importance of proper handling of mobile devices such as removable media;
- ensure that all members of staff are aware that their employment does not allow non-company devices to be used within the company network;
- use encryption software which enables centralised policy enforcement of strong encryption of all data stored at mobile devices and removable media;
- use policies to control the amount of login attempts that people may use to try and get at information they shouldn't;
- have methods in place which enables encrypted data to be decrypted in a controlled way outside the corporate network;
- the encryption process should be transparent and quick to the user, so that it does not interfere with their work or put any extra requirements on the user; and
- have methods (independent of the end user) which enable decryption of all encrypted data within the company network.

Pointsec argues that preventing people bringing removable media devices into the office is an extremely difficult problem. However, although they are fun and convenient, they are very easy to lose or abuse and therefore a real security threat. If companies are to prevent breaking new legislation such as Sarbanes Oxley, Basel 2, The Data Protection Act, as well as not falling victim to the havoc these tiny portable devices can cause, companies need to rapidly get to grips with the risks associated with removable media and protect themselves against these risks.

Editor's note

Further information from www.pointsec.com

United States

Distributors of ''file sharing'' software can be liable for secondary copyright infringement

Metro—Goldwyn—Mayer Studios Inc. v. Grokster Ltd (No. 04-480 US Supp. Ct. 27 June 2005)
The United States Supreme Court in a land mark ruling has held that one who distributes a device

with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. Justice Souter delivering the unanimous opinion of the court in respect of respondents Grokster Ltd. and StreamCast Networks Inc. (defendants in the original trial) who distributed free software products allowing computer users to share electronic files through peer-to-peer networks. These are so called because users' computers could communicate directly with each other, instead of through central servers. As such they needed no central computer server to mediate the exchange of information or files among users enabling high-bandwidth communication capacity to be dispensed with as well as the need for costly server storage space which was eliminated.

Background to the case

As well as their popular use for music distribution the benefits and security cost in efficiency meant that peer-to-peer networks were employed to store and distribute electronic files within universities, government agencies, corporations and libraries among others. Other users of peer-to-peer networks included individual recipients of Grokster's and StreamCast's software. Although the networks they enjoyed through using the software could be used to share any type of digital file, such users prominently employed those networks in order to share copyrighted music and video files without authorization. A group of copyright holders (MGM and others) sued Grokster and StreamCast for their users' copyright infringements, alleging that they knowingly and intentionally distributed their software to enable users to reproduce and distribute the copyright works in violation of the Copyright Act, 17 U.S.C. Section 101 et seq. MGM sought damages and an injunction.

Although Grokster and StreamCast did not know when particular files were copied a few searches, using their software, would show what is available on the networks the software reaches. MGM commissioned a statistician to conduct a systematic search and his study showed that nearly 90% of the files available for download on the FastTrack system were copyrighted works. Grokster and StreamCast disputed this figure and also argued that potential noninfringing uses of their software were significant in kind and even frequent in practice. As for quantification, MGM's evidence gave reason to think that the vast majority of users' downloads were in fact acts of infringement. It was also clear that well over 100 million copies of the software in question was known to have been downloaded and billions of files were being shared on the FastTrack and Gnutella networks that respectively supported the operation of the Grokster and StreamCast software.

Grokster and StreamCast conceded the infringement in those downloads and it was uncontested that they were aware that users employed their software primarily to download copyrighted files, even if the decentralised FastTrack and Gnutella networks failed to reveal which files were being copied and when. Following successful litigation against Napster Inc. by copyright holders in **A & M Records, Inc. v. Napster, Inc.** (114 F. Supp. 2d 896 ND Cal. 2000) (aff'd in part, rev's in part, 239 F. 3d 1004 CA9 Cir. 2001) StreamCast sought to attract large numbers of former Napster users consequent on that company being shut down by court order. The evidence that Grokster sought to capture the market of former Napster users was sparser but interesting since Grokster launched its own OpenNap system called Swaptor inserting digital code into its Website so that computer users using Web searching engines to look for ''Napster'' or ''free filesharing'' would be directed to the Grokster Website where they could download the Grokster software.

Finally, there was no evidence that either company made an effort to filter copyrighted material from users' downloads or otherwise to impede the sharing of copyright files. Although Grokster appeared to have sent emails warning users about infringing content when it received threatening notices from copyright holders it never blocked anyone from continuing to use its software in that way. StreamCast not only rejected another company's offer of help to monitor infringement, it blocked the Internet Protocol addresses of entities it believed were trying to engage in such monitoring on its networks.

Court rulings prior to Supreme Court

At first instance the District Court limited its consideration to the asserted liability of Grokster and StreamCast for distributing the current versions of their software, leaving aside whether either was liable ''for damages arising from past versions of their software, or from other past activities''. The court held that those who used the Grokster and StreamCast's Morpheus software to download copyrighted media files directly infringed MGM's copyrights, a conclusion not contested on appeal. But the court nonetheless granted summary judgment in favor of Grokster

and StreamCast as to any liability arising from distribution of the then current versions of their software. This gave rise to no liability in the court's view because its use did not provide the distributors with actual knowledge of specific acts of infringement.

This was affirmed by the Court of Appeals (380 F. 3d 1154 CA 9th Cir. 2004). In the court's analysis a defendant was liable as a contributory infringer when it had knowledge of direct infringement and materially contributed to the infringement. But the court read **Sony Corp. of America v. Universal City Studios, Inc.** (464 U.S. 417 1984) as holding that distribution of a commercial product capable of substantial noninfringing uses could not give rise to contributory liability for infringement unless the distributor had actual knowledge of specific instances of infringement and failed to act on that knowledge. In the Ninth Circuit's view the fact that the software was capable of substantial noninfringing uses meant that Grokster and StreamCast were not liable because they had no such actual knowledge owing to the decentralised architecture of their software. The court also held that the respondents did not materially contribute to their users' infringement because it was the users themselves who searched for, retrieved, and stored the infringing files, with no involvement by the defendants beyond providing the software in the first place.

Applicants MGM and many of the *amici* criticised the Court of Appeal's holding for upsetting a sound balance between the respective values of supporting creative pursuits through copyright and promoting innovation in new communication technologies by limiting the incidence of liability for copyright infringement:

''The more artistic protection is favored, the more technological innovation may be discouraged; the administration of copyright law is an exercise in managing the trade-off'' (see *Sony* at 442).

In the court's view the tension between the two values was the core subject of the case, with its claim that digital distribution of copyrighted material threatened copyright holders as never before, because every copy was identical to the original, copying was easy, and many people (especially the young) used file sharing software to download copyrighted works. The very breadth of the software's use would draw the public directly into the debate over copyright policy. On the one side there was concern that the use of copying songs or movies using software like Grokster's and Napster's fostered disdained copyright protection. This was offset by a different concern that imposing liability, not only on infringers but on distributors of software (based on its potential for unlawful use), could limit further development of beneficial technologies.

In weighing up the issue the argument for imposing indirect liability in this case was, however, a powerful one, given the number of infringing downloads that occurred every day using StreamCast's and Grokster's software:

''When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to delegate a distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement (see **In re Aimster Copyright Litigation**, 334 F. 3d 643, 645–646 CA 7th Cir. 2003).''

One infringed contributorily by intentionally inducing or encouraging direct infringement (see **Gershwin Pub. Corp. v. Columbia Artists Management, Inc.,** 443 F. 2d 1159, 1162 CA 2nd Cir. 1971). Vicarious infringement occurred by profiting from direct infringement while declining to exercise a right to stop or limit it (**Shapiro, Bernstein Co. v. H.L. Green Co.,** 316 F. 2d 302, 307 CA 2nd Cir. 1963). Although the Copyright Act did not expressly render anyone liable for infringement committed by another (See **Sony Corp. v. Universal City Studios** 464 U.S. at 434) these doctrines of secondary liability emerged from common law principles and were well established in law (id., at 486).

The Supreme Court's analysis

In analysing the issue the Supreme Court declared that it had dealt with secondary copyright infringement in only one recent case: ''because MGM has tailored its principal claim to our opinion there, a look at our earlier holding is in order.'' In **Sony Corp. v. University City Studios**, (supra) this Court had addressed the claim that:

''secondary liability for infringement can arise from the very distribution of a commercial product. There, the product, novel at the time, was what we know today as the videocassette recorder of VCR. Copyright holders sued Sony as the manufacturer, claiming it was contributorily liable for infringement that occurred when VCR owners taped copyrighted programs because it supplied the means used to infringe, and it had constructive knowledge that infringement would occur. At the trial on the merits, the evidence showed that the principal use of the VCR was for 'time-shifting' or taping a program for later

viewing at a more convenient time, which the court found to be a fair, not an infringing use (id., at 423—424)''.

There was no evidence, therefore, that Sony had expressed the object of bringing about taping in violation of copyright or had taken active steps to increase its profits from unlawful taping. However:

''Because the VCR was 'capable of commercially significant noninfringing uses', we held the manufacturer could not be faulted solely on the basis of its distribution. This analysis reflected a patent law's traditional staple article of commerce doctrine, now codified, that distribution of a component of a patented device will not violate the patent if it is suitable for use in other ways'' (see 35 U.S.C. Section 271(c); **Aro Mfg. Co. v. Convertible Top Replacement Co.**, 377 U.S. 476, 485 1964).

Where an article was ''good for nothing else'' but infringement, there was no legitimate public interest in its unlicenced availability, and there would be no injustice in presuming or imputing an intent to infringe. On the other hand the doctrine absolved the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limited liability to instances of more acute fault than the mere understanding that some of one's products will be misused. It left breathing space for innovation and vigorous commerce: ''The parties of many of the *amici* in this case think the key to resolving it is the **Sony** rule and, in particular, what it means for a product to be 'capable of commercially significant noninfringing uses' (**Sony** at 442)''.

MGM had advanced the argument that granting summary judgment to Grokster and StreamCast as to their current activities gave too much weight to the value of innovative technology, and too little to the copyrights infringed by users of their software, given that 90% of works available on one of the networks was shown to be copyrighted. Assuming the remaining 10% to be its noninfringing use MGM argued that this should not qualify as a 'substantial' use. The Court should therefore qualify Sony to the extent of holding that a product used ''principally'' for infringement did not qualify. Grokster and StreamCast replied citing evidence that their software could be used to reproduce public domain works and they pointed to copyright holders who actually encouraged copying. Even if infringement was the principal practice with their software today, they argued that the noninfringing uses were significant and would grow.

Findings on Sony

The Supreme Court agreed with MGM that the Court of Appeals had misapplied **Sony** which it read as limiting secondary liability quite beyond the circumstances to which the case applied. **Sony** had barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knew was in fact used for infringement. The Ninth Circuit had read **Sony's** limitation to mean that:

''whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it; it read the rule as being this broad, even when an actual purpose to cause infringing use is known by evidence independent of design and distribution of the product, unless the distributors had 'specific knowledge of infringement at a time at which they contributed to the infringement, and failed to act upon that information' (380 F. 3d at 1162)''.

Because the Circuit had found the StreamCast and Grokster software capable of substantial lawful use, it concluded on the basis of its reading of **Sony** that neither company could be held liable, since there was no showing that their software, being without any central server, afforded them knowledge of specific unlawful uses.

In the Supreme Court's view this reading of **Sony** was in error converting the case from one about liability resting on imputed intent to one about liability on any theory. Because **Sony** did not displace other theories of secondary liability, and because the Supreme Court had found that it was error to grant summary judgment to the companies on MGM's inducement claim, the court had not revisited **Sony** further as MGM has requested to add a more quantified description of the point of balance between protection and commerce when liability rested solely on distribution with knowledge that unlawful use would occur. In the Court's view it was enough to note that the Ninth Circuit's judgment rested on an erroneous understanding of **Sony** and to leave further consideration of the **Sony** rule for a day when that may be required.

The Court went on to say, however, that **Sony**'s rule limited the imputing of culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in **Sony** required courts to ignore evidence of intent if there was such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law. Thus, where evidence when

beyond the product's characteristics or the knowledge that it might be put to infringing uses and showed statements or actions directed to promoting infringement, **Sony's** ''staple-article'' rule could not preclude liability. The court interpreted this to mean that one who distributed a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, was liable for the acts of infringement by third parties. The court was mindful of the need to avoid trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential.

Mere knowledge or inducement

Just as **Sony** failed to find intentional inducement, despite the knowledge of the VCR manufacturer that its device could be used to infringe, so mere knowledge of infringing potential or actual infringing uses could not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premised liability on:

''Purposeful, culpable expression and conduct and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise''.

To satisfy this requirement MGM needed to adduce evidence which StreamCast and Grokster communicated an inducing message to their software users. The classic instance of inducement was by advertisement or solicitation that broadcast a message designed to stimulate others to commit violations. MGM claimed that such a message was shown in this case. It was undisputed that StreamCast had beamed onto the computer screens of users of Napster-compatible programs advertisements urging the adoption of its OpenNap program. This was designed, as its name implied, to invite the custom of patrons of Napster, then under attack in the courts for facilitating massive infringement. Those who accepted StreamCast's OpenNap program were offered software to perform the same services, which a factfinder could conclude would readily have been understood in the Napster market as the ability to download copyrighted music files. Grokster distributed an electronic newsletter containing links to articles promoting its software's ability to access popular copyrighted music. Anyone whose Napster or free file-sharing searches turned up a link to Grokster would have understood Grokster to be offering the same file-sharing ability as Napster and to the same people who probably used Napster for infringing downloads.

Assessing the evidence each company had shown itself to be aiming to satisfy a known source of demand for copyright infringement, the market comprising former Napster users. Second, the evidence of unlawful objective was given added significance by MGM showing that neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. While the Ninth Circuit had treated the defendants' failure to develop such tools as irrelevant because they lacked an independent duty to monitor their users' activities; ''we think this evidence underscores Grokster's and StreamCast's intentional facilitation of their users' infringement''. Third, there was a further complement to the direct evidence of unlawful objective. Both StreamCast and Grokster made money by selling advertising space, by directing ads to the screens of computers employing their software. As the record showed, the more the software was used the more ads were sent out and the greater the advertising revenue became. Since the extent of the software's use determined the gain to the distributors, the commercial sense of their enterprise turned on high-volume use, which the record showed was infringing. The unlawful use was therefore unmistakable.

In addition to intent to bring about infringement and distribution of a device suitable for infringing use, the inducement theory required evidence of actual infringement by recipients of the device, the software in this case. As the account of the facts indicated:

''there is evidence of infringement on a gigantic scale, and there is no serious issue of the adequacy of MGM's showing on this point in order to survive the companies' summary judgment requests. Although an exact calculation of infringing use, as a basis for a claim of damages, is subject to dispute, there is no question that the summary judgment evidence is at least adequate to entitle MGM to go forward with claims for damages and equitable relief''.

The Court concluded that, in sum, this case was significantly different from **Sony** and reliance on that case to rule in favor of StreamCast and Grokster was in error. **Sony** dealt with a claim of liability based solely on distributing a product with alternative lawful and unlawful uses, with knowledge that some users would follow the unlawful course. The case had struck a balance between the interests of protection and innovation by holding

that the product's capability of substantial lawful employment should bar the imputation of fault and consequent secondary liability for the unlawful acts of others:

''MGM's evidence in this case most obviously addresses a different basis of liability for distributing a product open to alternative uses. Here, evidence of the distributors' words and deeds going beyond distribution as such shows a purpose to cause and profit from third-party acts of copyright infringement. If liability for inducing infringement is ultimately found, it will not be on the basis of presuming or imputing fault, but from inferring a patently illegal objective from statements and actions showing what that objective was.''

There was substantial evidence therefore in MGM's favor on all elements of inducement, and summary judgment in favor of Grokster and StreamCast was in error. On remand, reconsideration of MGM's motion for summary judgment would be in order. The judgment of the Court of Appeals was vacated and the case remanded for further proceedings consistent with this opinion. Addition supporting judgments were issued by Justice Ginsburg with whom the Chief Justice and Justice Kennedy joined concurring and by Justice Breyer with whom Justice Stevens and Justice O'Connor concurred.

Information security forum warns that the cost of Sarbanes-Oxley compliance is at the expense of other security spending

A new report published by the Information Security Forum (ISF) warns that the cost of complying with the Sarbanes-Oxley legislation is diverting spending away from addressing other security threats. The global not-for-profit organisation says that many of its members expect to spend more than $10m on information security controls for Sarbanes-Oxley. The business imperative to comply also means that in many cases the true cost of compliance is unknown.

With increasing concerns about compliance, the new ISF report provides a high-level overview of the Sarbanes-Oxley Act 2002 and examines how information security is affected by the requirement to comply. The report provides practical guidance to address problematic areas in the compliance process. According to the ISF, these problem areas include poor documentation; informal controls and use of spreadsheets, lack of clarity when dealing with outsource providers and insufficient understanding of the internal workings of large business applications.

What's more the Act ignores important security areas that are extremely important when dealing with risks to information, such as business continuity and disaster recovery. This makes it important to integrate compliance into an overall IT security and corporate governance strategy.

Any Jones, ISF Consultant said:

''In the wake of financial scandals like Enron and WorldCom, the Sarbanes-Oxley Act was designed to improve corporate governance and accountability but has proved difficult to interpret for information security professionals. As neither the legislation nor the official guidance specifically mentions the words 'information security', the impact on security policy and the security controls that need to be put into place must be determined by each individual organisation in the context of their business. Additionally, for organisations whose business is not primarily financial for example, manufacturing or product-service industries, the diversion of information security attention from other risk areas to Sarbanes-Oxley compliance may lead to important business risks being neglected. It is important that Sarbanes-Oxley does not push organisations into following a compliance-based approach rather than a risk-based approach that may compromise information security. The ISF report helps companies to achieve compliance while also ensuring that they have the appropriate security controls in place.''

Editor's note

The full Sarbanes-Oxley report is one of the latest additions to the ISF library of over 200 research reports that are available free of charge to ISF Members. The Information Security Forum (ISF) was founded in 1989 and is a not-for-profit international association of over 260 organisations which fund and co-operate in the development of practical, business driven solutions to information security and risk management problems. The ISF undertakes a research programme, and has invested more than US$75 million over the past 16 years in providing best practice material for its members.

Further information from: www.securityforum.org.

US surveillance survey finds many companies monitoring, recording, videotaping and firing employees

From computer monitoring and telephone tapping to video surveillance and GPS satellite tracking,

employers are using policy and technology to manage productivity and protect resources. To motivate employee compliance, companies increasingly are putting teeth in their technology policies. Fully 26% have fired workers for misusing the Internet. Another 25% have terminated employees for e-mail misuse. And 6% have fired employees for misusing office telephones. That is according to the *2005 Electronic Monitoring & Surveillance Survey* from American Management Association (AMA) and the ePolicy Institute.

Internet, e-mail, IM and blogging

When it comes to workplace computer use, employers are primarily concerned about inappropriate Web surfing, with 76% monitoring workers' Website connections. Fully 65% of companies use software to block connections to inappropriate Websites — a 27% increase since 2001 when AMA and ePolicy Institute last surveyed electronic monitoring and surveillance policies and procedures in the workplace.

Computer monitoring takes various forms, with 36% of employers tracking content, keystrokes and time spent at the keyboard. Another 50% store and review employees' computer files. Companies also keep an eye on e-mail, with 55% retaining and reviewing messages.

Employers are doing a good job of notifying employees when they are being watched. Of those organisations that engage in monitoring and surveillance activities, fully 80% inform workers that the company is monitoring content, keystrokes and time spent at the keyboard; 82% let employees know the company stores and reviews computer files; 86% alert employees to e-mail monitoring; and 89% notify employees that their Web usage is being tracked. Commenting Nancy Flynn, executive director of the ePolicy Institute said:

''Concern over litigation and the role electronic evidence plays in lawsuits and regulatory investigations has spurred more employers to implement electronic technology policies. Workers' e-mail, IM, blog and Internet content creates written business records that are the electronic equivalent of DNA evidence.''

She noted that one in five employers has had e-mail subpoenaed by courts and regulators and another 13% have battled workplace lawsuits triggered by employee e-mail. She said:

''To help control the risk of litigation, security breaches and other electronic disasters, employers should take advantage of technology tools to battle people problems — including the accidental and intentional misuse of computer systems, telephones and other electronic resources''.

Telephone, cell phones, camera phones and voice mail

Concerned about inappropriate telephone use, 57% of employers block access to 900 lines and other unauthorized phone numbers. The numbers of employers who monitor the amount of time employees spend on the phone and track the numbers called has jumped to 51%, up from 9% in 2001. The percentage of companies that tape phone conversations has also grown in the past four years. In 2001, 9% of companies recorded workers' phone calls. Today, 19% tape the calls of employees in selected job categories, and another 3% record and review all employees' phone chat.

Far fewer employers monitor employees' voice mail messages, with 15% reporting that they tape or review voice mail. To help manage employees' telephone use, employers apply a combination of policy and discipline. Twenty seven percent have a written policy governing personal cell phone use at the office, and another 19% use policy to help control the capture and transmission of images via camera phones. Six percent of companies have fired employees for misusing office phones, and another 22% have issued formal reprimands to those who abuse phone privileges.

Video surveillance

More than half of the companies surveyed use video monitoring to counter theft, violence and sabotage (51% in 2005 vs. 33% in 2001). The number of companies that use video surveillance to track employees' on-the-job performance has also increased, with 10% now videotaping selected job categories and 6% videotaping all employees. Among companies that videotape workers, 85% notify employees of the practice.

Global satellite positioning and emerging surveillance technology

Employers have been slow to adopt emerging monitoring and surveillance technologies to help track employee productivity and movement. Employers who use Assisted Global Positioning or Global Positioning Systems satellite technology are in the minority, with only 5% using GPS to monitor cell phones; 8% using GPS to track company vehicles; and 8% using GSP to monitor employee ID/Smartcards.

The majority (53%) of companies employ Smartcard technology to control physical security and access to buildings and data centers. Trailing far behind is the use of technology that enables

fingerprint scans (5%), facial recognition (2%) and iris scans (0.5%).

Editor's note

The 2005 Electronic Monitoring & Surveillance Survey is co-sponsored by American Management Association (www.amanet.org) and the ePolicy Institute (www.epolicyinstitute.com). A total of 526 U.S. companies participated: 23% represent companies employing 100 or fewer workers, 101–500 employees (25%), 501–1000 (10%), 1001–2500 (13%), 2501–5000 (7%) and 5001 or more (22%).

Study into insider threat to computer systems published

A study into computer systems sabotage and critical infrastructure sectors has been conducted by the Secret Service National Threat Assessment Centre (NTAC) and the CERT program of Carnegie Mellon Universities' Software Engineering Institute. The insider effect study (ITS) focuses on the individuals who have access to information systems and have perpetrated harm using them. It examines each incident from the behavioural and the technical perspective. The study combines the Secret Service's expertise in behavioural and incident analysis with the CERT's technical expertise in network systems survivability and security. The ITS builds on earlier studies that focussed on identifying information that was operationally relevant and could help prevent future violent of disruptive incidents. The goal of the earlier research:

''was to find information that could help enhance threat assessment efforts — efforts to identify, assess, and manage the risk of harm an individual may pose, before the individual has the opportunity to engage in violent behaviour''.

The cases examined in the present insider effect study are incidents perpetrated by insiders (current or former employees or contractors) who intentionally exceeded or misused an authorized level of network, system or data access in a manner that affected the security of the organisations' data, systems, or daily business operations. The study finds that most of the insiders who committed acts of sabotage were former employees who had held a technical position with the targeted organisation. The majority of the incidents examined were perpetrated against private sector organisations. These caused financial losses, negative impacts to business operations and damage to reputation. As a result of these incidents almost all of the insiders were charged with criminal offences and the majority with violations of federal law.

Among the key findings of the ITS study are the following:

- negative work-event triggered most insiders' actions;
- most of the insiders had acted throughout in a concerning manner in the workplace;
- the majority of insiders planned their activities in advance;
- when hired, the majority of insiders were granted system administrative or privileged access, but less than half had authorized access at the time of the incident;
- insiders used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes and/or procedures, that relatively sophisticated attack tools were also employed;
- the majority of insiders compromised computer accounts, created unauthorized back door accounts, or used shared accounts in their attacks;
- remote access was used to carry out the majority of the attacks; and
- the majority of insider attacks were only detected once there was a noticeable irregularity in the information system or the system became unavailable.

Editor's note

Available from: www.secretservice.gov/ntac/its_report_050516_es.pdf

International

WIPO recommends uniform mechanism to regulate Domain NameRegistrations with introduction of new gTLDs

The World Intellectual Property Organisation (WIPO) has recommended the introduction of a uniform intellectual property (IP) protection mechanism designed to further curb unauthorized registration of domain names in all new generic Top-Level Domains (gTLDs). This comes in a report by WIPO's Arbitration and Mediation Center (WIPO Center) on the IP implications of introducing additional generic Top-Level Domains (new gTLDs). The report says that such a preventive mechanism would complement the curative relief provided by

the existing Uniform Domain Name Dispute Resolution Policy (UDRP).

The report is based on WIPO's experience in the area of IP protection in the domain name system (DNS). Commenting Mr. Francis Gurry, WIPO Deputy Director General who oversees the work of the Center said:

''The introduction of a new gTLD presents particular challenges for IP owners seeking to protect their domain names against unauthorized registration by third parties. With the growth of Internet usage and electronic commerce, the strategic importance of domain names as business identifiers has grown significantly.''

Mr. Gurry said that registering their entire trademark portfolio may often be the only way for IP owners to protect their identifiers from being ''grabbed'' by cybersquatters. If domain names are randomly attributed in newly opened gTLDs, IP owners will be forced to compete with cybersquatters for their own trademarks — unless additional safeguards are introduced, he added. ''Our new report makes practical recommendations for addressing such issues.''

WIPO's report has been prepared in response to a request made by the Internet Corporation for Assigned Names and Numbers (ICANN), the institution that oversees the functioning of the DNS. Following the introduction of seven new gTLDs in 2000 (.aero, .biz, .coop, .info, .museum, .name, .pro), ICANN is developing a comprehensive strategy for further expansion of the DNS. The report provides input into that strategy from an IP and dispute resolution perspective.

WIPO's recommendations made in the context of the First WIPO Internet Domain Name Process in 1999 led to the adoption of the UDRP — intended to offer a quick and cost effective procedure for the independent resolution of disputes that arise from the abusive registration of trademarks as domain names. Under the UDRP, a complainant must demonstrate that the disputed domain name is identical or confusingly similar to its trademark, that the respondent does not have a right or legitimate interest in the domain name and that the respondent registered and used the domain name in bad faith. The WIPO Center was the first UDRP service provider to be accredited in December 1999 and has since administered over 7500 cases under this policy alone. The WIPO Center has also been involved in the implementation of certain trademark protection mechanisms developed by new gTLD operators, and has handled more than 15,000 dispute resolution procedures under such mechanisms.

WIPO's report focuses exclusively on the IP aspects that need to be taken into account if and when such extensions of the domain name space take place, and does not comment on whether further extensions are necessary or desirable. The report summarizes the WIPO Center's UDRP experience, and notes that WIPO's UDRP case filing rate has remained stable over the last years and recently even increased. An additional mechanism to prevent unauthorized registration of domain names during the critical introductory phase of a new gTLD would, therefore, strengthen the ability to combat the still widespread practice of cybersquatting.

WIPO's UDRP experience also shows that the first extension of the DNS in 2000 has not caused significant shifts in cybersquatting or enforcement patterns. UDRP disputes continue to concentrate heavily in the .com domain. Indeed, this trend has become even more pronounced since the introduction of the seven new gTLDs. While this may partly be explained by the availability of the start-up IP protection mechanisms adopted by .biz and .info, it more likely indicates that .com continues to be the most attractive domain for trademark owners as well as for cybersquatters.

The report summarizes the WIPO Center's experience in implementing various IP protection mechanisms developed by a number of new gTLDs and provides a comparative evaluation of existing approaches (watch services, defensive registrations, exclusion mechanisms, and pre-registration mechanisms). It notes a trend among TLDs towards sunrise mechanisms, i.e. the possibility for IP owners to register their identifiers before the general public. Experience shows that the need for IP protection mechanisms is most tangible in open gTLDs, which are not subject to clearly defined and policed registration restrictions, and which accept domain name applications from the general public. The fewer restrictions and prior verification requirements associated with the registration process, the greater the risk of abusive registrations.

The report also confirms the need for effective IP protection mechanisms to prevent new gTLDs from turning into cybersquatting havens and recommends that mechanisms should: be effective and minimize the potential for abuse; take account of rights and interests of third parties; and be practicable and straightforward in order to avoid undue delays in the introduction or functioning of new gTLDs.

In conclusion, the report recommends implementing a single uniform preventive IP protection

mechanism across all new gTLDs. Specifically, new gTLDs would be required to offer IP owners the option of registering their protected identifiers during a specified period before opening registration to the general public. In sponsored or restricted gTLDs, where IP owners may not be eligible to register domain names, IP owners could instead be given the option of obtaining defensive registrations during this initial period. Such a uniform mechanism would have a number of advantages:

- operators of new gTLDs would not be required to develop their own IP protection mechanisms, a task for which they are not necessarily equipped;
- ICANN would not be required to monitor the correct implementation of multiple protection mechanisms applied by different gTLDs (now that ICANN's experimental ''proof of concept'' phase on new gTLDs has been concluded);
- IP owners would not be required to devote significant resources to understanding and using multiple different IP protection mechanisms; and
- the general public would benefit from enhanced reliability and credibility of domains.

Editor's note

The report, New Generic Top-Level Domains: Intellectual Property Considerations, is available from: http://arbiter.wipo.int/domains/reports.newgtld-ip

Online music distribution providing both opportunities and challenges according to OECD report

Online music distribution is set to grow significantly over the next few years, forcing industry to reconsider their business models and posing regulatory challenges to governments, according to a new OECD report on the digital music industry.

The rise of online music sales has implications for a wide range of players, including artists, consumers, the record industry, and new digital intermediaries. The OECD underlines the positive potential of digital distribution, both as a new business model and as a new social and cultural phenomenon. Its report also concludes that Internet-based piracy may be reduced, if licenced file-sharing and new forms of (super)-distribution evolve.

The report is the outcome of work involving of a wide range of stakeholders. It represents one of the first roadmaps as to how public policy should be re-evaluated.

In particular, the OECD calls for policies which balance the interests of suppliers and users, in areas such as the protection of intellectual property rights and digital rights management, without disadvantaging innovative e-business models and new technologies. Given that the online distribution of content is a relatively new phenomenon, legal frameworks involving issues such as rights protection technologies and secure (micro)-payment systems may need to be revisited.

Findings of the report include:

- Around one-third of Internet users in OECD countries have downloaded files from peer-to-peer (P2P) networks, with the number of simultaneous users on all P2P networks reaching almost 10 million users in October 2004.
- In principle, file-sharing software is an innovative and promising technology. However, many P2P users are making unauthorized copies not only of music, but increasingly also of video and software.
- It is difficult to establish a basis to prove a causal relationship between the 20% fall in overall revenues experienced by the music industry between 1999 and 2003, but digital piracy may be an important impediment to the success of legitimate online content markets.
- The year 2004 marked a turning point when a range of legitimate online music services became available. By the end of 2004, there were 230 sites offering over 1 m tracks online in the US and Europe.
- In the online business model, it is mainly the record labels that generate direct revenues from the sale of online music over third-party services. In the current environment, online music providers currently face low or zero margins, calling into question wholesale and retail pricing.
- Online music sales account for only a small share of total revenues (1—2%), but they are forecast to rise by a factor of 3—5 by 2008, representing 5—10% of revenue. In addition, there are positive and significant economic ripple effects on the consumer electronics manufacturers, the PC and telecom industries and on new digital intermediaries (e.g., digital rights management software).
- Efforts by value chain participants to vertically integrate some of the different functions along the value chain accompany the trend towards online music delivery.