

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION DEVELOPMENT BUREAU

E-STRATEGIES UNIT

**RESEARCH ON LEGISLATION IN DATA PRIVACY,
SECURITY AND THE PREVENTION OF CYBERCRIME**

OCTOBER 15, 2005

Disclaimer

This report is the result of research and analysis done by Ms. Michela Menting Yoell as part of her internship for an LLM law degree at the ITU/BDT E-strategies Unit with the objective of providing some guidelines to developing countries on legislation in data privacy, security and prevention of cyber crime. The opinions expressed are those of the authors and do not engage the ITU in any way.

PREFACE

Within the framework of WTDC-02 Istanbul Action Plan Programme 3 (E-Strategies and E-Services/Applications), ITU is mandated to assist Member States in developing laws and model legislation for e-services, prevention of cyber crime, security and data privacy. Within this context, Ms. Michela MENTING NOELL undertook research as an intern at ITU/BDT/E-Strategies Unit as part of her post-graduate work for an LLM Law Degree in Information Technology, Media and e-Commerce at the University of Essex in England.

The result of this internship is this report on Research on legislation in data privacy, security and the prevention of cybercrime which is aimed at assisting developing countries through the case studies included herein, analysis and research to provide guidelines on legislative issues that are part of the mandate of Programme 3.

ABSTRACT

The information age has made the public and private sectors of modern society increasingly dependent on technology, in which telecommunications play a vital role. Over the past thirty years, developed nations' transit from the industrial era to the new information age has enabled them to develop the nascent technology and produce ever greater quality in standards and value. The past decades have also delivered many opportunities in which the flaws and faults of the system have been exploited and mended, by hackers and legitimate users alike. The new society has engendered new types of crimes, such as phishing and botnets and facilitated the commission of old crimes, for example the violation of intellectual property rights, with new technology facilitating breaches of copyright in music, films and software. As society grows ever more reliant on these technologies, so does the concern for security, especially in cyberspace. The emancipation of the Internet has leaped ahead of the judicial system, but the authorities have taken heed and the wheels of the legal machine have started turning. The difficulty however has been that the Internet based society has no physical boundaries and thus much traffic escapes national supremacy. Therefore the need to look to an international framework would immensely facilitate regulation in this area. The European Union has enabled harmonized implementation of regulation on electronic commerce through directives in almost all European countries, with non-member countries aligning themselves with the EU movement. As founding father to the Internet, the US has both important knowledge and experience in the legal field of cybersecurity, with significant influence in the area. Developing countries are jumping onto the bandwagon. However, many of those countries are coming straight from an agricultural society and with the technological know-how of developed nations, are starting to create the infrastructure needed to support a technology based society. The problem is nonetheless that many have neither the expertise nor the experience to deal with the legal and policy issues necessary. In order to promote the development and use of technologies and the Internet, security must be assured, especially for e-commerce businesses. The International Telecommunication Union's Development Bureau mandate is to assist such developing countries to acquire the knowledge and develop the founding blocks for an information society. One of these founding blocks is cybersecurity. In order to compile general but adequate guidelines on such a vast area, research on existing legislation in developing countries and multinational frameworks is examined on both a content level, encompassing intellectual property, digital rights management and anti-circumvention, and a network security level, incorporating areas such as technical standards and integrity of data, with a close look at the security of information

infrastructure (privacy and data protection) and computer-related crimes (spamming and identity theft), among other topics.

ACKNOWLEDGEMENTS

I would like to thank Professor Rohan Kariyawasam, Law Lecturer at the University of Essex in the United Kingdom and Alexander Ntoko, Chief of ITU/BDT E-Strategies Unit for supervising my work, Bogdan Manolea, legal advisor at INTERNEWS in the RITI dot-Gov project at Romanian Information Technology Initiative (<http://www.legi-internet.ro/en/index.htm>) for his contribution on Romania and Peter Menting, Lawyer for the International Counsel Bureau in Kuwait for editing of the report.

TABLE OF CONTENTS

INTRODUCTION.....	7
1. INTELLECTUAL PROPERTY.....	13
Copyright & Digital Rights Management.....	13
Trademark & Domain Name.....	21
Hypertext Linking.....	28
Framing.....	30
Metatagging.....	31
2. NETWORK SECURITY.....	33
Authentication.....	33
Access Control & Communication Security.....	47
3. SECURITY OF INFORMATION INFRASTRUCTURE.....	56
Data Security, Privacy & Confidentiality.....	56
Availability.....	76
4. CYBERCRIME.....	84
Fraud.....	88
Phishing.....	92
ID Theft.....	95
Insider Fraud.....	96
CONCLUSION.....	101
BIBLIOGRAPHY.....	104

INTRODUCTION

Today's digital age is rapidly becoming congruent with almost all aspects of modern societies. While dependence on information systems grows, so does the use of such systems span out to reach the most isolated places around the world. Proliferation of computers and reliance on these systems becomes a global phenomenon, enlarging the information infrastructure linking these different systems together, becoming more complex and more difficult to manage at a centralized level without impeding on speed and quality. The inherent nature of the Internet obliterates all physical boundaries and thus becomes an international network of information systems, serving all kinds of functions, be they public or private, profit-making or simply the gratuitous dissemination of information.

The use of information and communication technologies (ICTs) is always expanding, with the number of users growing exponentially each year. Between 2000 and 2005, the average Internet user growth rate was of 146.2%, the highest rate being in the Middle East with 266.5%. Not far behind were Latin America and the Caribbean with 211.2% and Asia with 198.3%.¹ It is clear from these statistics that these regions, in which most developing countries subsist, are eager to implement and exploit the advantages of ICTs and the Internet superhighway.

Clearly the benefits of a technology-based society are keenly sought by developing nations, seeking a boost to their national economy with the enhanced processing speed of information, productivity and efficiency that information systems enable. This significantly reduces costs, which is immensely attractive to businesses and government entities alike. With a minimum amount of investment needed, adequate knowledge, and readily available information, electronically based service businesses can easily be set up as compared to the more traditional type of industry and agriculture of the past century. This is extremely attractive for developing countries, which often find it difficult to compete on the worldwide market against corporate giants based in Europe and North America. Inevitably, the growth of ICTs leads to the increasing importance of the telecommunications sector, which has become the backbone for information transmission and storage.

This globalisation of ICTS has however a posed a problem regarding its security. The growth of information networks and Internet usage means that decentralization and interconnectivity take on a global aspect, multiplying the points of potential vulnerabilities of the system. Vulnerabilities are not only found in the technical nature of the infrastructure but also in the users themselves. The greater the

¹ Internet Usage Statistics - The Big Picture: World Internet Users and Population Stats, www.InternetWorldStats.com
Copyright 2005, Miniwatts International, LLC.

number of users of information systems, the greater the number of system failures due to human errors. Risks of loss can occur at different levels, from unauthorized access and use, misappropriation and modification or simply from the destruction of information systems, either accidentally or voluntary. As technology becomes available to even the most modest users, so does the concern for security of the infrastructure and protection against risk of loss or interference become ever more important. Cybersecurity denominates the need to secure cyberspace, the Internet as well as closed networks. Information systems do not radically change from one country to another, therefore any fault or failure found in one particular system will inevitably affect similar systems found in any other part of the world. This is particularly the case with Microsoft's Windows, which is the most used operating system worldwide, with almost 90% of the market.

Consequently, any flaws inherent in the software will unavoidably affect operating systems everywhere. Exploitation of intrinsic flaws to the system is common among the Internet underworld of hackers. The increasing sophistication of hacking tools, along with their propagation and the diffusion of information about system weaknesses on the Internet unavoidably leads malicious crackers with decreasing levels of computer knowledge to utilize them and try to cause damage on a global scale. Flaws exist in certain components of Windows's interface, with exploits for the vulnerabilities publicly available on the net. Viruses and worms such as My Doom, Bagel or even Netsky manipulate the flaw to enable attack from a remote user. The speed in which these viruses spread and multiply is incredible and widespread infection is attained in a matter of hours. As a result security is an important concept and must be applied consistently and internationally for it to have an impact that is relevant in the global network.

Malicious programmers based in countries where laws dealing with Internet crime are slow to develop, are out of reach of the authorities. This was the case of the I Love You virus creator who caused pandemonium in information systems in 2000. Living in the Philippines, authorities were unable to charge the creator because a relevant law with which to prosecute him under did not exist. More recently, the Philippines have put into place legislation dealing with Internet crime, however it cannot be retroactively applied. This supervirus nonetheless caused millions of dollars in damages worldwide, and prosecution of this crime was not possible. Faced with barriers of national boundaries, the US and Europe were unable to bring the perpetrator to justice for damage caused to their information systems. It is therefore imperative to harmonise international laws as much as possible when dealing with Internet related crimes.

An important element in securing cyberspace, is addressing the threats and vulnerabilities present and potential. International cooperation and discussion is imperative in order to keep within the pace of technological developments. At present, many viruses and variations exist which can corrupt files in a system causing irreparable damage. It is vital that appropriate legislation be put into place in those countries where development of information infrastructure is already launched and electronic commerce is still in its early stage. In order to adequately protect the information technology fledglings of developing nations, a secure base in their ICTs as well as knowledge and guidance in the field is essential.

The International Telecommunication Union (ITU) is a United Nations agency where governments and private sector coordinate global telecom networks and services. The Telecommunication Development Bureau is charged with connectivity and access, fostering policy, regulatory and network readiness, expanding human capacity through training programs, formulating financing strategies and e-enabling enterprises in developing countries.² The ITU/BDT/E-strategies Unit assists developing countries in harnessing the potentials of ICTs to contribute towards reducing the social divide, improving the quality life, promoting universal access and facilitating entry into the information society.³ One of the principal objectives is helping developing countries to establish a legislative framework for regulating the Internet.

The World Summit on the Information Society (WSIS) which took place in December 2003 in Geneva lay down a Declaration of Principles and a Plan of Action⁴ to promote a clear statement of political will and take concrete steps to establish the foundations for an Information Society, reflecting all the different interests at stake.⁵ The WSIS objectives should be looked at in conjunction with the mandate adopted by the ITU-D at the World Telecommunications Development Conference (WTDC) of 2002, from which the Istanbul Action Plan Programme 3 (IsAP) was set up. It addressed security, confidence and e-legislation in two of its six priority areas. One of the most pertinent aims was to provide assistance to Member States in developing laws and model legislation for e-services/applications, prevention of cybercrime, security, ethical issues and data privacy.

² International Telecommunication Union website, <http://www.itu.int/ITU-D/>

³ ITU-D: E-Strategy Unit website, <http://www.itu.int/ITU-D/e-strategy/>

⁴ Section C5 of the Plan of Action underlines the importance of building confidence and security in the use of ICTs. Cooperation between the private sector, governments and the different Member Countries in prevention, detection and recovery is stressed, as well as the encouragement of further development of secure and reliable applications.

[The Declaration of Principles states](#) *“that strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. In order to achieve this, a global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies.”* ITU WSIS Thematic Meeting on Cybersecurity website, <http://www.itu.int/osg/spu/cybersecurity/index.phtml>

⁵ World Summit on the Information Society website, <http://www.itu.int/wsisis/basic/about.html>

It is clear that one of the ITU-D's main aim in assisting developing countries concerns cybersecurity and e-legislation. A stable and secure foundation in both the infrastructure and in the legislation is necessary for the development of further online services and transactions. In order for a country to be able to securely oversee ICT progress and growth, a firm legislative structure needs to underlie it. Only in this way can effective control and remedial processes be endorsed legitimately, and sanctions against variants enforced. ICTs are moving forward like a huge waterfall and the direction of the current cannot be reversed. However, the pace of the waterfall may be controlled by the construction of a dam, with filtering and speed restraint. Not all particles of water can be scrutinized, nevertheless big debris and the like can be blocked. This is analogous to ICTs and specifically the Internet. The amount of security needed should ideally be proportionate to the value of the information that is being stored or transmitted. Therefore over-legislating in this area would lead to a reduction in effectiveness, speed and quality.

Even so there are certain aspects of ICTs that need protection from a legislative point of view, especially regarding existing legislation on data security and intellectual property rights, as well as old forms of crimes being committed on the new information superhighway, such as fraud and extortion. Clearly the legislature needs to be revised and adapted to ICTs, as well as recognizing that new types of computer-related crimes exist and new security devices are needed to authenticate information flows.

This report will address the legislative imperatives needed to protect national interests of developing nations and assure the development of ICTs and electronic commerce, while securing the infrastructure with adequate legislative protection. Three pervasive principles have become acknowledged as important components of cybersecurity. These are confidentiality, integrity and availability. The three issues have overlapping areas, which are very closely related. It is sometimes difficult to draw a fine line between the different categories and to determine which type of legislation would adequately cover a specified area. Cybersecurity can however be delimited into two distinct topics: content and network security.

Content refers to the actual subject matter of the information transmitted. In this category, intellectual property rights (IPR), namely copyright and domain names, can be coupled with digital rights management (DRM) and anti-circumvention techniques. The importance of the legal entitlement to exercise rightful control over the use of an IP should not be undermined by the massive surge of online piracy. It is perhaps more pertinent to look at new and evolving IP legislation as it will be more applicable to the digital economy. Is it possible for developing nations to follow in the same line as the US and the EU when addressing issues such as DRM and anti-circumvention technologies? The

essential point here is to determine the effect in developing countries that such legislation could have if not properly implemented or misunderstood. This is essentially important as IPRs could potentially stifle cultural as well as technological development in favour of monopolistic entertainment industries. Priorities in developed countries are not always the priorities of developing nations and as such, especially regarding trademark issues and anti-piracy measures, existing legislation in developed countries needs to be adapted to the needs of developing states.

Network security is also a key element in cybersecurity. It relates to the security of the infrastructure, its legitimate use, the transactions taking place online and the integrity of the data that is being transmitted or stored. Technical standards need to be addressed, such as access control and communication security. This is to ensure the stability of the infrastructure for all users, especially for e-commerce. The reliance on a secure network is extremely important if e-commerce is really to take off in developing nations. This also raises the matter of security for network-based transactions. Finally, and most importantly, the integrity of data must be ensured if confidence is to be built up. The value of the infrastructure is worth nothing if it cannot establish security in relaying information.

Accordingly, research into the legislation already surrounding data security, protection of privacy, confidentiality and authentication using tools such as encryption, Public Key Infrastructure (PKI), digital and e-signatures, is crucial. An analysis of computer-related crime, or cybercrime, and the legislation surrounding it can very much help to establish a thorough and stable framework for sanctioning. Cybercrime is an important issue that needs to be addressed fairly quickly by developing nations. The problem is that many malfeasors on the Internet base themselves in developing countries precisely because there are no laws under which such crimes can be prosecuted. Countries in Eastern Europe and Asia are ripe terrains for the new Internet mafia, as the laws in some of these countries do not proscribe many online criminal activities. The US and the EU have not had *gain de cause* in many cases as actions such as the creation of malicious software and viruses remains out of reach of the law and thus of extradition procedures.

There is the additional problem related to e-commerce. Such commerce is seen as a breakthrough for developing countries to lessen the gap to the information society. The real issue at hand centres on the creation of an ideal market place for e-commerce to take off, strengthened by a firm legislative base and at the same time a framework liberal enough to allow a positive and rapid development of e-commerce services. Concerns regarding Internet service providers as well as certification providers for PKIs need to be addressed in a context that is specific to developing nations. Applying developed

nation's legislative models on liability might prove too burdensome for developing ISPs, slowing down and perhaps even deterring development of e-commerce and related services.

Without forgetting the ITU-D's mandate and priorities, this report is aimed at assisting developing countries to address the requirements for elaborating legislation in the domain of cybersecurity. Lessons can be learned from existing legislation in developed nations. However, such legislation cannot be directly applied to developing states since their context is often completely different from the one where such legislation was born. It should also be kept in mind that, although the contexts may be radically different, legislation on certain matters, mainly regarding authentication, confidentiality and privacy should be harmonized as best as possible to avoid future conflicts of law. The inherent nature of the Internet is a global one, and therefore security in this domain should be as standardized as possible on an international level.

1. INTELLECTUAL PROPERTY RIGHTS

COPYRIGHT & DIGITAL RIGHTS MANAGEMENT

Intellectual Property Rights and related legislation has become an important source of protection on copyrighted material since the advent of digital media and the immense facility with which such media can be reproduced, shared and distributed internationally. Most concerned with such protection is by far the entertainment industry. The music and film industries have tapped a ubiquitous market in the form of the Internet. Global sales of recorded music amounted to a total of US \$33.6 billion in 2004, while digital sales multiplied by 10 between 2003 and 2004 with approximately 200 million tracks downloaded in 2004.⁶ This growth subsists, non-withstanding the numerous file-sharing programs and websites, which enables people to trade and download such media for free.

Two treaties, negotiated under the auspices of the World Intellectual Property Organization (WIPO), the **Copyright Treaty of 1996** (Annex 1) and the **Phonograms & Performers Treaty of 1996** (Annex 2) attempt to interpret traditional rules of copyright in the new Internet environment. New elements have been added to the conventional methods of protecting copyrights, namely through the introduction of the legal protection of technological anti-circumvention measures, placed on digital media so as to disallow unauthorized reproduction.

⁶ Global music retail sales, including digital, flat in 2004: London, March 22 2005. Adrian Strain, Julie Harari or Fiona Harley at IFPI Communications. http://www.ifpi.org/site-content/publications/rin_order.html

The International Intellectual Property Alliance emphasizes the importance of these two treaties as they enable the development of electronic commerce and facilitate access to scientific, medical and technical data, educational materials, and technical and productivity software. Trade in these resources results in prosperity and provides its users with a competitive advantage. Commerce is cheaper, more efficient, and easier in a digital networked marketplace.⁷ Not only does commerce in data attract a lot of investment in technology based information trade, but also helps strengthen a country's cultural and creative industries.

In the 1980s, a survey of intellectual property laws in developing countries revealed that many laws were mere replicas of their colonizing countries,⁸ and became eventually inadequate with the advent of the new information age. It has been recognized that good intellectual property laws in developing countries can stimulate creativity and inventiveness, contributing to the society's development. Additionally, it can attract domestic and foreign direct investment in its entertainment, cultural and educational industries, enabling protection of traditional folklore and culture. Such development also allows for expansion of the infrastructure necessary for the manufacture and distribution in these industries.⁹

Both WIPO Treaties have been implemented in the US, the European Union (EU), Canada and other countries with mitigated effects. The **Information Society Directive** (Annex 3) of the European Union¹⁰ has concretely implemented the right of reproduction and the right of communication, whereas the United States' **Digital Millennium Copyright Act of 1998** (Annex 4) (DMCA) states that such a right can be interpreted directly from the Treaties without the need to recreate these rights in US law. Titles I and II of the DMCA effectively implement both WIPO treaties but only explicitly stipulate limitations and exceptions to the rights of reproduction and communication. Both these rights are implied by the fact that the DMCA explicitly states the implementation of the WIPO treaties. The difficulty in applying copyright protection to the digital world is the ease and perfection with which such media can be burned, copied, transferred and shared between computers, portable media and the Internet. The INDICARE project, a European Consumer Survey launched in 7 European countries on

⁷ International Intellectual Property Alliance: The WIPO Treaties http://www.iipa.com/wipo_treaties.html

⁸ A Developing Countries Perspective By Betty Mould-Iddrisu, Chief State Attorney, International Law Division, Ministry of Justice, Ghana, International Information Programs, www.usinfo.state.gov/products/pubs/intelprp/perspect.htm

⁹ Ibid

¹⁰ EU Copyright Directive 2001/29/EC

Digital Music Usage and Digital Rights Management showed that 69% of Internet users had already gained a first experience with digital music on their computers.¹¹

United States

The US, under pressure from the big entertainment industries, has adopted stricter copyright laws with regards to digital media and anti-circumvention measures. When the movie industry started releasing media in Digital Versatile Disk (DVD) format, it did so only after the US enacted the DMCA in 1998, which granted legal protection to anti-circumvention measures.¹² However, the Net act preceded the DMCA, which also dealt with copyright and criminalized infringement.

The US **No Electronic Theft Act of 1997**¹³ (NET Act) (Annex 5) made copyright violation a criminal act.¹⁴ The NET Act could be applied to the unauthorized trading of infringing [MP3](#) files, although music [file sharing](#) was yet not widely practiced in 1997. The infringements of greatest interest to the industry at that time were primarily copies of [software](#).¹⁵

In the US case of *Sony-Betamax*, the Supreme Court established the rule that manufacturers and distributors of mass-market technology for a variety of uses¹⁶ may not be subjected to liability for distribution of the products to the general public so long as their products are “merely capable of substantial non infringing uses.”¹⁷

The court in [A&M Records v. Napster](#)¹⁸ upheld the Sony-Betamax decision. The plaintiff record companies filed suit alleging contributory and vicarious federal copyright infringement and related state law violations by defendant Napster, Inc. Napster was an online file sharing network where users could download for free files shared by other users in return for sharing files on the network. The court however drew a distinction between the Napster software and the architecture of its system, on the one hand and Napster’s conduct, namely its operation of a file-indexing service, on the other hand.¹⁹ The

¹¹ [Digital Music Usage and DRM: Results from a European Consumer Survey](#) by Nicole Dufft, Andreas Stiehler, Danny Voageley, Thorsten Wichmann, May 24, 2005. Indicare: The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe.

¹² *No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.*

¹³ amended section 506(a) of title 17 of the US Code

¹⁴ **CRIMINAL INFRINGEMENT-** Any person who infringes a copyright willfully either-- "(1) for purposes of commercial advantage or private financial gain, or "(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$ 1,000 shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.'

¹⁵ http://en.wikipedia.org/wiki/NET_Act

¹⁶ staple articles of commerce

¹⁷ *Mtrea-Glodwyn-Mayer Studios Inc. et al. V Grokster Ltd.* US District Court, California, [2002], lines 15 - 19

¹⁸ 239 F.3d 1004 (9th Cir. 2001)

¹⁹ *Supra* 1, lines 24 - 26

court '*place[d] the burden on plaintiffs to provide notice to Napster*' and imposed on Napster the responsibility '*of policing the system within the limits of the system.*'²⁰ Therefore the onus is on the plaintiff to alert Napster of infringing uses on the network, and once Napster receives reasonable knowledge of abuse, then it must act expediently to remove those infringing files from its index.

Digital Rights Management (DRM) is a general term that refers to copy control mechanisms used to control or restrict the use of digital media on electronic devices.²¹ These mechanisms sometimes make use of cryptography and encoding technologies in order to prevent copyright violation and piracy. Anti-circumvention laws effectively prohibit technologies, which to all intents and purposes allow a user to circumvent copy protection techniques.

The US's DMCA effectively sought to crack down on online violation of intellectual property rights in film, music and publications brought about by the massive surge in use of peer to peer sharing networks in the late 1990s. Section 1201 (a)(1)(A)²² makes it illegal to circumvent a technological measure that controls access to a work protected by intellectual property. Section 1201 (a)(2)(A)²³ further makes it illegal to participate in the manufacture, import, offer to the public, provision or traffic of anti-circumvention technologies.

Specific problems have been found in the DMCA, which was intended to stop copyright pirates from defeating anti-piracy protections added to copyrighted works.²⁴ Section 1201 effectively bans *acts* of circumvention as well as the *distribution* of tools and technologies used for circumvention. US case law however has shown that the Act has unfortunately had a negative effect on scientific research in fields related to anti-circumvention technologies.

In *US v Elcom Ltd. aka Elcom Co. Ltd. & Dmitry Sklyarov*²⁵, a foreign programmer working for a company based in Russia was arrested on the allegations that a software program he had developed for his employer effectively removed restrictions embedded into Adobe's e-book program contrary to section 1201 of the DMCA. The programmer was eventually released but the US is currently pursuing his employer, Elcom Ltd on similar charges.

²⁰ The UCLA Online Institute for Cyberspace Law and Policy. A&M Records v. Napster: [MP3 File Sharing Disputes Continue in the Aftermath of Recent Court Rulings](http://www.gseis.ucla.edu/iclp/napster.htm), <http://www.gseis.ucla.edu/iclp/napster.htm>

²¹ http://en.wikipedia.org/wiki/Digital_rights_management

²² No person shall circumvent a technological measure that effectively controls access to a work protected under this title.

²³ No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of [circumventing](#) a technological measure that effectively controls access to a work protected under this title.

²⁴ Electronic Frontier Foundation: Unintended Consequences: Five Years under the DMCA www.eff.org

²⁵ U.S. District Court Northern District of California, May 8, 2002. 203 F.Supp.2d 1111, [62 USPQ2d 1736](#)

Threats of litigation under the DMCA have also been made against legitimate university research based in the US. The case of Professor Felten did not come to court, primarily because the research team decided to abstain from presenting their findings on certain watermarking technologies intended to protect digital music. The researchers wanted to discuss their findings and publish a scientific paper about the vulnerabilities of several technologies they had studied. Such publishing often results in improved technology and enhanced consumer choice. The irony of the case essentially comes from a public challenge issued by Secure Digital Music Initiative encouraging skilled technologists to try and defeat their technology. Professor Felten and his research team from Princeton University took up the challenge and effectively managed to defeat the technology. They were however deterred from revealing their findings at a scientific conference by threat of litigation under section 1201 of the DMCA.

The DMCA has inadvertently had the effect of restricting research into security flaws found in copy-protection mechanisms. The importance of research in this domain is essential for the advancement and evolution of these technologies. Publication of findings enables improvement and security. Consequently, it is important to ensure that while anti-circumvention laws need to be put into place in order to clamp down on Internet piracy, such measures should not hinder research into related technologies.

European Union

In the EU, the **European Directive 2001/29/EC**²⁶ of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights (EUCD) provides directions for implementation of anti-circumvention measures, while at the same time trying to safeguard research initiative.

Paragraph **48** of the Directive clearly states that the legal protection conferred on anti-circumvention technologies “*should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography*”. Article **3(a)** stipulates that Member States may provide for exceptions to the rights when the purpose is for teaching or scientific research.

²⁶ Annex 3

However it has been noted in a critique of the proposed UK implementation of the EU copyright directive²⁷ that several aspects have been left uncovered and need to be addressed. The critique was a response to a consultation process launched by the UK Patent Office. The critique looks at flaws in the Directive and at some of the problems the DMCA has posed in the US, making recommendations for a solution.

Protection of research has also been underlined in the paper and some proposals have been made. Firstly, there is a need to protect researchers against prosecution so that cases such as Dmitry Skylarov's and Professor Felten does not undermine scientific research. Protection should also be granted for publication of information in furtherance of research into cryptography as well as bona-fide publications. The critique stresses that both commercial and non-commercial forms of research publications should be allowed. Additionally, protection should extend to include persons who are not academics but who are nonetheless experts and sufficiently trained in the field to warrant contributive knowledge. The critique also suggests that the legislation should ideally define encryption research and permissible technologies on a basis that is "*reasonably calculated to advance the state of knowledge or development of encryption technologies*".

Reverse engineering for the purposes of interoperability is important for the use of digital media on different operating systems. Under the DMCA, **Section 1201 (f)(1)**²⁸ allows for reverse engineering of an anti-circumvention measure but only for the achievement of interoperability of an independently created computer program. However, the interoperation must not already be available. This means that if reverse engineering has already been accomplished once for interoperability purposes, then such an action cannot be undertaken again.

Reverse engineering however is not only used for interoperability. Other activities may also have a legitimate need to reverse engineer certain products, for example, manipulating the computer code of a digital toy to make it perform new functions, disabling an access control device on the storage media of an entertainment product, creating a patch for a software program or electronics product or even performing cryptanalysis on security systems that control access to digital data. Such a control seems however to be too strictly limited. Different methods enabling reverse engineering might prove to be

²⁷ Critique of the Proposed UK Implementation of the EU Copyright Directive by Julian T. J. Midgley (jtjm@ukcdr.org), Campaign for Digital Rights: <http://ukcdr.org/issues/eucd/ukimpl/>

²⁸ Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

more efficient and therefore limiting reverse engineering in such a way might not be conducive to developing efficient interoperability.

The US case of *Universal v Eric Corey & 2600 Enterprises Inc*²⁹ is a good example of the limitations imposed on software programming. The case concerned the posting on the Internet of a decryption program executable on Microsoft operating systems which enabled the playback of copy protected DVDs on players that did not have the player keys necessary to enable decryption of the digital media contained on the DVD. Records show that the program was originally created in order to allow interoperability of the DVD's with Linux operating systems, which at the time were unable to play the copy-protected DVDs.

The EU CD does not propose any possible solution either, although it is up to Member States to put into place compatible legislation. Julian Midgley, in his critique paper, points out that this enables software companies to exert complete control over the creation of interoperable products that can only be created with knowledge obtained from decompilation of their programs.³⁰ Limitation on the possibilities for reverse engineering might inadvertently lead to anti-trust practices or abuse of a dominant position. It is therefore necessary to ensure that anti-circumvention measures do not prevent the decompilation of computer programs and do not hinder competition policies as already established.

DRMs are seen as very controversial in developed countries. It is important that these countries ensure that foreign rights holders not impede on national copyright law, especially exceptions and limitations of such legislation. Additionally, foreign rights holder's anti-circumvention technologies should not have the effect of curbing second-hand legal sale and re-sale of copyrighted works, since the import of cultural and educational materials is a significant source of commerce for developing nations.³¹

The INDICARE European Consumer Survey³² outlines in its conclusion that consumers are not willing to give up flexibility. They want to burn, share and store music files on their computers and are willing to pay more for an unprotected version of a work. Thus interoperability is the key demand from users. It is crucial therefore that commercial digital music offering must ensure that their applied DRM systems support these demands.³³

²⁹ No. 00-9185 (2d Cir. 2001)

³⁰ Supra 16

³¹ INDICARE: DRM and developing countries by Manon Ress, Washington DC, USA on 29/04/05

³² The INformed Dialogue about Consumer Acceptability of DRM Solutions in Europe, http://www.indicare.org/tiki-view_articles.php

³³ Digital Music Usage and DRM: Results from a European Consumer Survey by Nicole Dufft, Andreas Stiehler, Danny Vogeley, Thorsten Wichmann, May 24, 2005. Indicare: The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe.

Canada

Perhaps a better example of up-to-date legislation is the Canadian Legal Framework, where the Copyright Board of Canada declared Peer to Peer downloading to be legal in 2003. The decision was based on the fact that users are not always aware of whether their downloads are copyrighted or not. The liability shifts to the users uploading the media, as they should be more informed as to whether the content they are sharing is copyrighted or not.

Canada has additionally focused on the imposition of levies on recordable media, such as blank DVDs, CDs, MDs, and MP3 players, as well as removable storage media. Proceeds go to music content owners through the Canadian Private Copying Collective, a collecting society-cum-trade association for the Canadian music industry.³⁴ Canada's proposed C-60 Bill which will reform its copyright laws, would put into law the decision of the Copyright Board of 2003.

DRM protection varies enormously depending on the legal framework of a country. Common law jurisdictions such as the US, Australian, the UK and former British colonies, do not confer blanket rights on consumers regarding the use of copyrighted works. They rely on the notions of Fair Dealing or Fair Use laws, where the interest of the consumer is balanced against that of the infringing act. However, in Civil law jurisdictions such as France, the Appeal Courts held in April of 2005 that copy prevention software on DVDs violated privacy rights of consumers to make copies of recordings purchased for personal use.³⁵ The case was brought before the French courts by consumer advocacy group UFC-Que Choisir on behalf of a man who wanted to make a VHS copy of a DVD for a relative's videocassette player. France, along with Germany and Spain, for instance, have laws that guarantee the right of consumers to make copies of recordings they have purchased for private use, even though EU copyright law allows copy-protection measures to be applied to products. Such a stark contradiction will inevitably lead to decisions such as the one made by the Parisian court.

The problem that has been raised with anti-circumvention technologies is that of the expiry of the copyright. When this happens, the copyrighted work usually falls into the public domain. However, there is no guarantee in the current legislation in place in the US and in the EU that media, which has fallen into the public domain and which is stored on devices containing copy-protection technology, would allow legitimate circumvention of the technology. Copyright protection has a lifespan of about 50 to 70 years, depending on the country. As an ephemeral protection, anti-circumvention laws should

³⁴ [Canada Declares P2P Downloading Legal](http://www.drmwatch.com/legal/article.php/3290471) December 18, 2003 By [Bill Rosenblatt](#),
<http://www.drmwatch.com/legal/article.php/3290471>

³⁵ [Associated Press: Court Rules Against DVD Copy Preventions](#), Tuesday April 26, 6:11 pm ET
By Mary Maccarthy, Associated Press Writer

lapse with the expiry of the copyright. Therefore it is necessary that provisions for the release of media into the public domain should be put into place, especially when this would mean bypassing copy-protection technology on digital media. In the EU CD critique, Midgeley suggests that such work also be available in an unprotected form, so as to guarantee the passage into public domain once copyright has expired. This would also entail granting archivists and librarians an unprotected copy of the media or special exemptions from anti-circumvention laws.

The legal protection of anti-circumvention technology should also not undermine the practices of music studios, manufacturers and distributors who frequently copy and sample digital media. Possession of devices incorporating mechanisms to circumvent copy-protection measures in the course of a business should not create a criminal liability. Manufacture, sale, possession, distribution, etc of circumvention devices should be a civil offence only. Therefore an exception should be made for the use of circumvention technologies for music studios, manufacturers and distributors.

TRADE MARK & DOMAIN NAME

A domain name corresponds to the Internet-Protocol (IP) address of a computer, which is represented by a string of numbers. The user-friendly 'translation' of the IP address into a unique name of a computer or website is a domain name. A domain name, like IP addresses, differentiates one computer or network from other networks on the Internet.³⁶ Domain names can designate an address, such as a specific organization or a trademark, for example amazon.com. A trademark is the symbol (or word, phrase, logo, etc.) used by a company to distinguish its products from those of another. If one company uses another's trademark as its domain name, under UK and US law this effectively qualifies as trademark infringement, depending on the registration and use of the trademark. This protection of trademark ownership in domain names is also afforded to companies where the sale of products is connected with the domain name, precluding other companies from using that domain name as their trademark.

Cybersquatting refers to the practice of buying domain names with the intent of selling them back to the companies who already own the trademark.³⁷ This practice does not deal exclusively with companies, but can also concern famous individuals and other non-profit entities. The intent of the perpetrator is primarily to make use of the other person's good name to make a profit, either by selling back the domain name or by selling products and services under the assumed trademark. Domain names have proved extremely valuable to businesses ever since the take off of electronic commercial

³⁶ <http://www.nolo.com/definition.cfm/Term/3E9F8AE7-B46F-40A6-9E737BBFA8FDAE75/alpha/D/>

³⁷ <http://www.nolo.com/definition.cfm/Term/AA9AABDE-3C77-4868-B9D329BC68205E50/alpha/C/>

transactions. The opportunity to reach a global market almost instantaneously has been snatched up by established multi-nationals. In order to successfully establish a presence on the World Wide Web, for these companies, it is important that their domain name match that of their trademark, in order for them to be easily found on the net. Domain names are also crucial for start up web companies which build their reputation online and therefore through their domain name. Usurpers of trademarks and domain names can be potentially harmful for the business both financially and reputation-wise. As trademarks and domain names are increasingly associated together on the net, so does the need for adequate legal protection regarding abusive acquisition and use of domain names need to be put into place in order to safeguard legitimate business activities.

International

The Internet Corporation for Assigned Names and Numbers (ICANN), headquartered in the US, is the administrator of the domain name system (DNS) internationally, accrediting a number of national registrars of domain names. The WIPO Administrative Panel decided the very first case to be presented under the new ICANN Domain Name Dispute Resolution Policy (Annex 6) in February 2002. Under the Policy, dispute proceedings arising from alleged abusive registrations of domain names (for example, cybersquatting) may be initiated by a holder of trademark rights. Section 4.b(1) effectively deals with evidence of registration and use in bad faith.³⁸

The case was that of *Telstra Corporation Limited v. Nuclear Marshmallow*.³⁹ The complainant was an Australian company, Telstra Corp. The respondent was an unregistered company, Nuclear Marshmallows. The respondent had effectively registered telstra.org in the US, of which the contact name was an unidentifiable person. Telstra Corp, an international company and the largest to be listed on the Australian stock exchange, had already registered many variant domain names of Telstra (telstra.com, telstra.net, etc). The Panel considered the respondent's identity and activities. It concluded that the respondent had an identical domain name to the trademark of Telstra, and thus the domain name was confusingly similar to Telstra's other domain name registrations. The Respondent had not provided evidence of rights or legitimate interests in the domain name and the Panel found that the domain name was registered and used in bad faith since the respondent did not conduct any legitimate commercial or non-commercial activity under the registered domain name, and the

³⁸ For the purposes of [Paragraph 4\(a\)\(iii\)](#), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith: (i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name;

³⁹ Case No. D2000-0003

Respondent took deliberate steps to conceal its true identity.⁴⁰ The Panel considered that the passive holding of the domain name amounted to the respondent acting in bad faith, in the circumstances of this particular case.⁴¹

The protection of legitimate trademarks in the new online environment is a delicate matter for legal consideration. A trademark is a distinguishing mark representing a company which has invested in it substantially in order for consumers to be able to recognize and associate the company's specific products and services to a particular mark. Trademarks represent the reputation of a company and its business. Usurping such a trademark essentially amounts to usurping that company's reputation and good name. This undermines the company, as it is not able to control the quality of products or services being offered by the infringer to consumers. Trademark law thus protects the company against infringement and abuse of its reputation by third parties.

Domain name on the other hand does not necessarily represent a company's trade. It is just an online identifier of any person or entity who chooses to operate a website. However, with the surge of electronic commerce, and the vast potential of online consumer shopping, companies are registering their trademarks as domain names. With a limitless number of potential consumers surfing the web and searching for information about certain companies, it is very likely that searches are undertaken using a company's trademark. Until the year 2000, domain name authorities were registering domain names on a first come first serve basis, meaning that anyone could register any name, including trademarks. Many cybersquatters started registering famous names and making a commercial business out of selling these domain names to companies who owned the trademarks. This proved problematic for the value of trademarks in general. With the growing importance of e-commerce, domain names were to prove as valuable as trademarks. Consequently ICANN's new domain name dispute resolution policy tackled the problem of abusive registrations of domain names by enabling the holder of trademark

⁴⁰ Extract from the conclusions of the administrative panel decision at the WIPO arbitration and mediation center <http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0003.html>

⁴¹ The particular circumstances of this case which lead to this conclusion are:

- (i) the Complainant's trademark has a strong reputation and is widely known, as evidenced by its substantial use in Australia and in other countries,
 - (ii) the Respondent has provided no evidence whatsoever of any actual or contemplated good faith use by it of the domain name,
 - (iii) the Respondent has taken active steps to conceal its true identity, by operating under a name that is not a registered business name,
 - (iv) the Respondent has actively provided, and failed to correct, false contact details, in breach of its registration agreement, and
 - (v) taking into account all of the above, it is not possible to conceive of any plausible actual or contemplated active use of the domain name by the Respondent that would not be illegitimate, such as by being a passing off, an infringement of consumer protection legislation, or an infringement of the Complainant's rights under trademark law.
- In light of these particular circumstances, the Administrative Panel concludes that the Respondent's passive holding of the domain name in this particular case satisfies the requirement of paragraph 4(a)(iii) that the domain name "is being used in bad faith" by Respondent."

rights to initiate litigation against the domain name holder. Protection of trademark reputation is an important issue, especially in the online environment where the potential of e-commerce businesses is enormous.

United States

The US case of *Intermatic Inc. v. Dennis Toeppen*⁴² (pre-ACPA) was one of many trademark infringement claims made against Toeppen, a US citizen who had reserved approximately 240 domain names of famous trademarks (such as Delta Airlines, British Airways, Panavision and in this case Intermatic) with a view to reselling these domain names back to the trademark owners. Intermatic claimed that Toeppen did not have permission to register these domain names. However, Toeppen stated that he did not need to ask authorization as domain name registration was not a misuse or dilution of trademark. Despite the lack of legislation on the subject, the Court nonetheless found that registration of domain names with the only intent of making a business of selling them to trademark owners constituted in fact malicious intent to profit from a trademark by using domain name registration as a bypass. Toeppen and his associates were consequently enjoined from using the trademark in any way and from using the domain name intermatic.com. This and subsequent Toeppen cases eventually led the way to the drafting of the Anticybersquatting Consumer Protection Act which came into force in 1999.

Under the **Anticybersquatting Consumer Protection Act of 1999** (ACPA) (Annex 7), the purchase of a domain name similar to an existing trademark by a person who is not the trademark owner is a practice effectively classed as trademark infringement. Trademark dilution (using a variant form of a registered trademark) is also a prohibited practice under the **US Federal Trademark Dilution Act** (Annex 8). This law adds [section 43\(d\)](#) to the **U.S. Trademark Act of 1946** and creates a cause of action for "cybersquatting" famous trademarks. The ACPA also creates a federal cause of action for cybersquatting a person's name without her permission.⁴³

Under the ACPA, cybersquatting is illegal since it breaches the fundamental rights of the trademark owner to use her trademark.⁴⁴ However, the trademark is only infringed if it existed at the time of the domain name registration. Speculative reservation of domain names is legitimate.

⁴² No. 96 C 1982. United States District Court, N.D. Illinois, Eastern Division. Nov. 26, 1996

⁴³ Copyright © 1999-2001 Submerged Ideas, Inc. Anticyberquatting Consumer Protection Act <http://www.submerged-ideas.com/litigation/anticybersquat.htm>

⁴⁴ [Cybersquatting and Trademark Infringement](#) by Monica Kilian, University of Melbourne, E Law – Murdoch University Electronic Journal of Law, Vol 7, No 3 (September 2000)

In order for a plaintiff to bring a successful action against a cybersquatter, she must prove that the defendant has a bad faith intent to profit from that trademark, including a domain name which is protected as a trademark. The defendant must have registered, trafficked in, or used a domain name identical or confusingly similar to a mark.⁴⁵

The ACPA provides a non-exhaustive list of factors to aid in the determination of what constitutes bad faith.⁴⁶ It is important to note that bad faith will not be found if the Courts believe that the defendant had reasonable grounds to believe that the use of the domain name was lawful and acted in good faith.

Another US case, *Jack in the Box Inc. v. jackinthebox.org and jackinthebox.net*⁴⁷, reinforced the *in rem* jurisdiction procedure for cybersquatting. The provision allows for plaintiffs to sue infringing domain names rather than the person or company who registered it. Such a condition was allowed for the ACPA because of the difficulty of tracking down cybersquatters who often register under false names or who reside outside US territory.

In this case, the court transferred back the two domain names at .net and .org to the claimant namely because no one was present to defend the registered domain names. The real issue of the case was whether mere registration of the domain names, without actual use of the names to create a website,

⁴⁵ Keyt Law: Business, Internet, E-commerce & Domain Name Law. Domain Name Disputes FAQ: The Anticybersquatting Consumer Protection Act, by Richard Keyt April 20, 2001.
<http://www.keytlaw.com/urls/acpa.htm#What%20is%20the%20ACPA?>

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark.

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

(III) is a trademark, word, or name protected by reason of (the Red Cross, the American National Red Cross or the Geneva cross) or 36 U.S.C. § 220506'.

⁴⁶ The trademark or other intellectual property rights of the defendant, if any, in the domain name;

1. the extent to which the domain name consists of the legal name of the defendant or a name that is otherwise commonly used to identify the defendant;
2. the defendant's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
3. the defendant's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
4. the defendant's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
5. the defendant's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the defendant's prior conduct indicating a pattern of such conduct;
6. the defendant's provision of material and misleading false contact information when applying for the registration of the domain name, the defendant's intentional failure to maintain accurate contact information, or the defendant's prior conduct indicating a pattern of such conduct;
7. the defendant's registration or acquisition of multiple domain names which the defendant knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and
8. the extent to which the mark incorporated in the defendant's domain name registration is or is not distinctive and famous within the meaning of Section **Error! Hyperlink reference not valid.** of the Lanham Act.

⁴⁷ 143 F. Supp. 2d 590, 592 (ED. Va. 2001)

was enough to uphold a claim in trademark infringement. Chief District Judge Claude M. Hilton stated that:

*"A domain name registrant need not actually develop a working Web site for the illegal use of the mark to constitute commercial use. [...] The act of registering a domain name is a commercial act because it involves a sale between the registrant and the registrar. The infringing domain name is used in this commercial act because it itself becomes the good or service that is sold."*⁴⁸

It is consequently possible for US courts to have *in rem* jurisdiction under the ACPA and therefore be able to apply traditional trademark law to the realities of cyberspace. This provision would most certainly prove to be detrimental to registrants who have legitimately registered a domain name, but for whatever reason, have not yet used the name commercially. The idea that a registrant must make use of the domain name within a certain confine of time contradicts what Judge Hilton has stated to be a legitimate commercial good. It would mean that a validly acquired good must be made use of commercially and publicly to become legitimate private property.

European Union

In the EU, two instruments are applicable to cybersquatting, the **EU Trademark directive**⁴⁹ (Annex 9) and the [EU Regulation 733/2002](#) (Annex 10), of which Article 5.1(b) concerns public policy on speculative and abusive registration of domain names including the possibility of registration of domain names in a phased manner to ensure appropriate temporary opportunities for the holders of prior rights recognized or established by national and/or Community law and for public bodies to register their names.

The EU is currently implementing an .eu top level domain name and is at present still working on a future Directive concerning cybersquatting. However it does look to the US ACPA, as well as the common law in the UK, and draft legislation being prepared in Belgium and Italy.

United Kingdom

The European Directive on Trademarks has pushed the UK to strengthen its trademark law. The UK has used the directive to confer protection against cybersquatting as well.

In the UK, in *Harrods v UK Network Services Limited and Others*⁵⁰, although an unreported case since the defendant was not present at the hearing, the court granted Harrods an injunction against Network

⁴⁸ Supra 21

⁴⁹ No. 89/104/Eec

⁵⁰ Chancery Division, 9 December 1996 (unreported) *The Times*, 2/12/9

Solution for having registered the domain name harrods.com. The court stated that registration of the domain name constituted trademark infringement and the common law tort of passing off. The judgment however is not reasoned, as the defendant had not actually made use of the domain name, so as to make doubtful the claims of infringement and passing off.

However one of the first actual cases concerning cybersquatting, with intent to profit, is that of *BT v One in a Million Ltd*⁵¹ & *Marks and Spencer v One in a Million Ltd*⁵². One in a Million was a company whose main business was registering domain names and selling them to interested parties. The company had effectively registered quite a few famous trademarks, such Marks & Spencer, Ladbrokes, Sainsburys, Virgin and British Telecom (BT). BT and others brought an action against One in a Million for trademark infringement and passing off. The court took the following factors into consideration, among all the other circumstances: the similarity of the names, the intention of the defendant and the type of trade.

The court accepted that the mere registration of a misleading domain name did not itself amount to a misrepresentation sufficient to establish passing off. However, the court ruled that there was a threat of misrepresentation where the defendants were offering to sell the misleading domain names to others for them to use, and thereby putting an instrument of deception or instrument of fraud into the hands of others. The court ruled that the elements of passing-off were considered to be present and that there was trademark infringement in terms of section 23 of the **United Kingdom Trade Marks Act 1994** (Annex 11).⁵³

Europe

Other countries have initiated a move to draft legislation in this domain. In Italy, a Draft Act on the **Regulation of the use of names to identify Internet domains and online services** will address personal names, identical or similar names to trademarks, distinctive signs and intellectual work, names of institutions or public authorities, geographical places and confusing or misleading names.

Similarly in Belgium, a draft law prohibiting abusive registration and providing criminal penalties and injunctions in case of registration of a domain name identical or similar to a trademark or service mark to gain an illegal advantage is being put into effect.

⁵¹ Court of Appeal, 23 July 1998 (unreported)

⁵² [1998] unreported 23/7/98

⁵³ Trademarks, domain names and patents by M Viljoen, GM du Plessis, G Vivier Beng, Partners at Adams & Adams, Pretoria. <http://www.buys.co.za/publications/cyberlaw/frbibliography.htm>

HYPERTEXT LINKAGES, FRAMING & METATAGGING

Hypertext Linking

Hypertext linking allows direct access from one website to another, without having to search for the website on a browser or type in an address in the URL (Uniform Resource Locator). Deep linking allows access to a web page inside the same or another website, bypassing the website's homepage. Although there is no existing legislation regarding linking, case law in the US and in Europe have litigated the legality of linking to different sites. Issues of copyright infringement and linking to sites containing illegal material have posed some problems, which the courts have decided differently in different jurisdictions.

United States

The very first cases are to be found in the US. In *Ticketmaster Corp. v Tickets.com*,⁵⁴ Ticketmaster Corp sued Tickets.com alleging that the deep links on Tickets.com's website leading to Ticketmaster constituted copyright infringement for hypertext linking. Federal Judge Hupp concluded that "*hypertext linking does not itself involve a violation of the Copyright Act...since no copying is involved*".⁵⁵ Hypertext linking does not involve the reproduction, distribution or preparation of copies or derivative work, therefore there was no infringement of copyright, since the link was one to the original author's website.

Europe

In the UK, the Shetland Times Limited brought an action against Dr Jonathan Wills & Another.⁵⁶

The Scottish court here granted an interlocutory injunction restraining the use by the defendants of a deep link to a number of the plaintiff's web pages. The issue at hand here concerned deep linking and whether such links to internal or embedded pages of the Shetland Times' web site by the Shetland News through the use of the plaintiff web site's news headlines was an act of copyright infringement under the United Kingdom's Copyright Designs and Patents Act of 1988.⁵⁷ Eventually the Shetland News agreed not to deep link to the Times's website, but instead to link directly to the Times's front web page.

⁵⁴ (99-7654)

⁵⁵ 000 B.C. Intell. Prop. & Tech. F. 040401. Internet Ruling: Hypertext Linking does not violate Copyright. Elijah Cocks, Staff Writer. http://www.bc.edu/bc_org/avp/law/st_org/iptf/headlines/content/2000040401.html

⁵⁶ 1997 F.S.R. (Ct. Sess. O.H.), 24 October 1996

⁵⁷ Netlitigation: Internet Law: News, Suits and Discussions, by Sugarman, Rogers, Barshak & Cohen, Linking, Framing and Metatagging. <http://www.netlitigation.com/netlitigation/cases/shetland.htm>

In Denmark, The Danish Newspapers Publishers Association⁵⁸ sued an Internet search engine for news, Newsbooster, alleging copyright violation by “deep linking” directly to articles on Danish Newspaper’s Internet sites. The Danish Court effectively ruled that such deep links violated the intellectual property rights of the claimants.

A similar judgment was reached in France in *Havas et Cadre On Line c/ Keljob*⁵⁹. Havas and CadreOnline were two Internet based companies advertising job offers online. They brought an action against Keljob concerning Keljob’s deep links to CadreOnline’s database, modification of CadreOnline’s source codes, presenting CadreOnline’s web pages under another URL and altering the navigation and logo of CadreOnline’s website. The Court effectively ordered Keljob to cease immediately as it did not have any legitimate rights to advertise CadreOnline’s web pages and database as it’s own.

Additional linking cases follow in the same line of reasoning. Unavoidably, linking to sites that offer illegal or copyright infringing material⁶⁰ including anti-circumvention software⁶¹ as well as pirated media files⁶² has also been ruled as illegal linking or contributory to copyright infringement.

Japan

In March 2000, in the Japanese Kuichi case, the Osaka District Judge held that linking to a website which contains illegal material can make the person placing those links chargeable with the offences of aiding and abetting under the Japanese Penal Code. This is regardless of the knowledge of the person placing these links,⁶³ pursuant to Japanese belief that ignorance of the law is no excuse. A harsher penalty was sought to deter illegal websites.

Germany

Nonetheless, some jurisdictions such as in Germany have been more favourable to hypertext linking than its European counterparts. A first decision by the Germany Federal Court of Justice ruled in 2003 that Paperboy⁶⁴, an online search engine, neither violated copyright nor competition law.⁶⁵ Similar to the Danish Newspapers Publishers Association case, the German Courts stressed the importance of

⁵⁸ Danish Newspaper Publisher’s Association v. Newsbooster, Decision of July 5, 2002, Copenhagen Bailiff’s Court

⁵⁹ TRIBUNAL DE COMMERCE DE PARIS 26 décembre 2000 <http://www.juriscom.net/txt/jurisfr/da/tcparis20001226.htm>

⁶⁰ Dutch case of [Court of Appeal in The Hague](#), Scientology v. Providers and Karin Spaink, Decision of September 4, 2003

⁶¹ Links to websites that sell infringing devices can violate the Digital Millennium Act, Comcast of Illinois X LLC v. High-tech Elec. Inc., [District Court for the Northern District of Illinois](#), Decision of July 28, 2004, 03 C 3231

⁶² Norwegian case of [The Circuit of Eidsivating](#), Decision of March 3, 2004, Napster.no

⁶³ [Cyberlaw India: To Link or Not to Link-The Judicial View](#) by Shri Pavan Duggal, Cyberlaw Consultant, President Cyberlaws.net, MAC, ICANN <http://www.cyberlaws.net/cyberindia/linking.html>

⁶⁴ BUNDESGERICHTSHOF 17. Juli 2003Walz Justizamtsinspektor als Urkundsbeamter der Geschäftsstelle ZPO § 253 Abs. 2 Nr. 2

⁶⁵ [Deep links are legal in Germany. Official](#) By [Drew Cullen](#) Published Sunday 20th July 2003 22:52 GMT

http://www.theregister.co.uk/2003/07/20/deep_links_are_legal/

linking to the internet and refused to concede to the view that web surfing should start at the homepage of every website. It also stated that if web site owners did not want other sites to deep link to their inner pages, then it was up to them to put into place technological barriers. A second case in 2004, the *Schöner Wetten* decision by the German Federal Court of Justice in Karlsruhe [issued a verdict](#) holding that an online service which offers links to articles in a protected database is not in violation of copyright and competition law, thus confirming the legality of deep links in Germany.⁶⁶

It should be noted, however that the new European parliament and council directive (2001/29/EC) on the harmonization of certain aspects of copyright and related rights in the information society might change this position as it questions whether the new right to make available material of the copyright holder potentially violates hyperlinking. It has yet to be seen what outcome the directive will have on Member States.

Framing

Framing is a more problematic issue than linking as of yet. It concerns framing a separate, often unrelated website inside a frame of another site. This means that the website framing the contents of another website, can advertise on the headers and sidebars of the frame, while displaying content from another website.

United States

In the US case of *The Washington Post, et als. v. TotalNews, Inc., et als*⁶⁷, the plaintiffs brought an action for copyright and trademark infringement based on the defendant's use of framing technology. TotalNews had effectively identified and advertised its name on the frames showing other news services website contents. The matter was eventually settled out of court and a linking agreement was reached whereby the Washington Post and other news services agreed to let TotalNews display simple links to their websites, but prohibited the use of frames, graphics, video or audio materials, or plaintiffs' proprietary logos, any or all of which might imply an affiliation with or endorsement of TotalNews by the plaintiffs.⁶⁸

⁶⁶ Links & Law - Information about legal aspects of search engines, linking and framing: The German Federal Court of Justice rules on the liability for hyperlinks, Update 18: June 11, 2004 <http://www.linksandlaw.com/news-update18.htm>

⁶⁷ 2001 Southern District of New York, Civil Action Number 97-1190.

⁶⁸ Supra 34

Another case to follow in the same line of reasoning was *Futuredontics Inc. v. Applied Anagramic Inc.*⁶⁹ Anagramic had effectively framed the content of a competing site, including its trademark in the frame as well as links to all of its web pages. A district court ruled that such framing modified the appearance of the linked site and could amount to infringement if authorization was not sought.

Metatagging

Meta-tags are information embedded into the HTML source of a Web page.⁷⁰ Indexing is a practice undertaken by search engines which index the text contained in web pages and permit users to search the index for key words or concepts.⁷¹

One of the first cases to deal with metatagging was the US case of *Playboy Enterprises, Inc. v. Calvin Designer Label*.⁷² Playboy enterprises successfully brought an action against Calvin Designer Label on allegations of trademark infringement, unfair competition and dilution. The defendant had used the trademark Playboy repetitively in the meta-tag of it's website so that when search engines indexed key words such as Playboy, the Calvin Designer Label contained a large amount of the searched term and would thus come up as one of the more popular websites. The courts granted a preliminary injunction against the defendants enjoining them from using the trademark Playboy in their metatags.

In light of the difficulties concerning intellectual property rights and the online environment, cross-linking agreements have become a safe way to avoid litigation by ensuring that permission to hyperlink is granted beforehand contractually. These agreements are license agreements between two web parties allowing each to hyperlink from his own website to the other's site. Such agreements become more and more attractive as they can cover use of trademark and copyright in both hyperlinking and framing. This is probably the safest approach for the moment, since different jurisdictions differ on the legality of such methods, and as legislation crystallizes itself, such agreements can provide safer means to manage and run websites, be they commercial or non-profit. Although it is clear that linking can sometimes be in breach of copyright and trademark law, it is of essence to the diffusion of information, enabling quick and easy access from one site to another and thus saving a lot of time researching and surfing for relevant information in the vast expanse that is the Internet.

⁶⁹ 1997 46 USPQ 2d 2005 (C.D. Calif. 1997)

⁷⁰ <http://en.wikipedia.org/wiki/Metatag>

⁷¹ <http://www.virtulaw.com/e-law.htm> This page was designed by Virtulaw, L.L.C. Copyright © 1999 Virtulaw, L.L.C. All rights reserved. Revised: June 04, 1999.

⁷² 985 F.Supp. 2d 1220 (N.D. Cal. 1997)

Nolo.com⁷³ software and website development urge developers to seek permission for linking in the following areas in order to avoid problems: deep links that bypass a linked site's home page, graphic links comprised of trademarks from the linked site, links that result in framing, and IMG links that pull only certain elements from a site (such as an image). The website development company adds that in the case where permission has not been sought or granted, legal disclaimers should be placed on the website so as to reduce the chance of liability for violation of intellectual property rights.

⁷³ <http://www.nolo.com/article.cfm/objectID/C13F7E6B-B05E-43DF-80D62B635DF9DD9F/>

2. NETWORK SECURITY

AUTHENTICATION

Authentication is the process that establishes the origin of the information or determines an entity's identity.⁷⁴ This comprises the use of smart cards, biometric identification, role-based technologies and e-signatures. Cryptography is often used in authentication processes, which is a coding method in which data is encrypted (translated into an unreadable format using a key) and then decrypted (translated back into a readable format with a corresponding key) using an algorithm.⁷⁵ This is the practice of encryption.

Public-key cryptography is a form of modern cryptography which allows users to communicate securely. It seems to be emerging as the prioritised framework for the implementation of electronic signatures in computer network communications and transactions.⁷⁶ It is an attractive authentication method since it allows for secure use on open networks. The appeal of public key cryptography is due namely to the fact that the parties communicating over an open network need not have previously exchanged their private keys. An entity wishing to communicate with another over the network will publish a public key while keeping the other key private. The sender will apply the private key algorithm to encrypt the message. The recipient will then get a hold of the public key and decrypt the message. If the decryption is successful, the recipient will know that the message is authentic and has been sent by the only person who retains the private key, the sender. In order to ensure confidence in the validity of public key cryptography, it is supported by a public key infrastructure. The Public Key Infrastructure (PKI) is maintained by trusted third parties, otherwise known as Certification Service Providers (CSP) which are certification authorities. CSPs ensure that the public key pertaining to an entity or an individual's private key is valid and has not been corrupted. Thus they verify the relationship between the identity of the expected signatory and his public key through the issuance of certificates confirming that the public key is effectively a valid key for that signatory. Revocation lists exist, on which public keys that are out of date or corrupted are listed. CSPs ensure trust in the use of public key cryptography.

⁷⁴ National Institute of Standards and Technology Computer Security: Recommendation for Key Management – Part 1: General (Glossary of Terms and Acronyms) by Elaine Barker, William Barker, William Burr, William Polk and Miles Smid. NIST Special publication 800-57, April 2005

⁷⁵ Intell recovery: Data recovery Definition, <http://www.intellirecovery.com/glossary/c.html>

⁷⁶ Electronic Law Journals – JILT 2003 – Public Key Infrastructure, Digital Signatures and Systematic Risk by Jamie Murray, Liverpool John Moores University

With the proliferation of information technology networks and the increasing popularity of electronic commerce, the electronic medium is slowly attaining the same level of importance as the paper medium. From a legal point of view, this means that electronic documents in commercial transactions need to be recognised as legally valid in the eyes of the law. The problem that such validation faces is the security of electronic documents. Easily tampered with and corrupted, potentially by the sender of the documents as well as by malfeasors intercepting communications, recognition of electronic documents has been treated with utmost caution by courts of law when determining their authenticity. However with cryptography and the PKI system, authenticity of messages can be effectively guaranteed. This means that electronic documents can be digitally signed by the sender so as to ensure their legitimacy. Digital signatures are becoming analogous to ordinary hand-written signatures. They are the result of a cryptographic transformation of data that, when properly implemented with supporting infrastructure and policy, provides the services of origin authentication, data integrity and signer non-repudiation.⁷⁷ A distinction must be made with electronic signatures, which refers to any mechanism for identifying the originator of an electronic message, not necessarily using cryptographic techniques.⁷⁸

Consequently with the improved security of digital signatures as applied to electronic transactions and communications, the admissibility of such signatures in a court of law has become a mandatory step for many countries, especially in the US and the EU. As such techniques become more and more widespread, such recognition needs to extend to all participating countries in electronic transactions.

Developing countries that wish to participate fully in electronic commerce must elaborate legislation in this domain if they wish to trade electronically with other countries. Minimum standardization is necessary in the domain of electronic and digital signatures law in order to ensure not only their authentication while contracting electronically, but also to guarantee legal recognition and enforceability of such contracts in court. The Philippines, for example, has enacted important legislation in this area with the **Electronic Commerce Act of 2000**, **Implementing Rules of the E-Commerce Act of 2000**, **Access Devices Regulation Act**, BSP Circular on Electronic Banking, and **Supreme Court Rules on Electronic Evidence 2001** (Annex 12). Guidelines for the Establishment and Operation of Information Technology (IT) Parks strongly encourages the development of IT involved in processing and transmitting information which include computing, multimedia, telecommunications, microelectronics, and their interdependencies in parks. Such parks house business

⁷⁷ Supra 1

⁷⁸ Wikipedia, The Free Online Encyclopedia

in a wide range of different online activities, which can be undertaken by any entity. Safeguards are put into place to ensure adequate infrastructure conducive to the smooth functioning of such activities.⁷⁹

International

Inspired by the OECD Guidelines, which advanced key principles on governing emerging PKI, the United Nations Commission on International Trade Law (UNCITRAL) adopted a model law which develops a legal framework for CSPs within an internationally operative PKI,⁸⁰ called the UNCITRAL Model Law on Electronic Signatures (2001) and which is accompanied by a Guide to Enactment of the **UNCITRAL Model Law on Electronic Signatures 2001** (Annex 13).

Article 2 of the Model law defines electronic signatures as “*data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message.*” This definition contains the three main aims of e-signatures which are the electronic form of the signature, the identification of the signatory and the non-repudiation of the signature, effectively ensuring that the signatory cannot later refute having signed the document.

⁷⁹ REGISTRABLE ACTIVITIES - IT Parks shall serve as locations for the following PEZA registrable activities:

1. Software development for business, e-commerce, education and entertainment;
2. Content development for multimedia or internet purposes;
3. Hardware design, prototype production and related activities;
4. Knowledge and computer-based support service activities such as, but not limited to, the following:
Regional/worldwide software support, Data encoding and conversion, Internet facilitation, Systems integration, Project implementation, IT consultancy Call centre
5. Research and development services;
6. Other related IT and computer-based services/activities as may be identified and approved by the PEZA Board;
7. Manufacturing facilities for IT Parks outside NCR.

INFRASTRUCTURE REQUIREMENTS - Developers of IT Parks shall install sufficient infrastructures and utilities to ensure that IT service exporters shall have access to the following:

1. High-speed fibre-optic telecommunication backbone and high-speed international gateway facility or wide-area network (WAN);
2. Clean, uninterrupted power supply;
3. Computer security and building monitoring systems (e.g., computer firewalls, encryption technology, fluctuation controls, etc.);
4. IT Research and development centre and educational facilities; and
5. IT business and technology incubation centres which will provide prospective locators not only with ready-to-occupy physical facilities for office and production spaces but also services needed by IT service exporters (e.g., secretarial, communications, administrative and other support services).

The IT Park may also provide facilities and services catering to the needs of IT service exporters, and their executives and personnel, as follows:

1. Executive and staff housing/accommodations;
2. Conference facilities, seminars/training/exhibit rooms and other facilities and services for business group activities;
3. Physical fitness, health improvement, medical and sport facilities;
4. Facilities and services for social and recreational activities; and
5. Other facilities that complement the IT community’s educational, social and cultural requirements.

⁸⁰ Supra 3, pag e 7

Article 6⁸¹ of the Model Law sets out the requirements for a signature. The three main issues in this model law are the recognition firstly that electronic signatures are legally valid if the signature data is undoubtedly linked to the signatory and no one else, secondly that at the time of creation such data was under his sole control and thirdly that any alteration made to the electronic signature must be detectable. Once these three sub articles are assured, then additional legal requirements for a signature may be put into place by the country wishing to adopt such legislation, as long as these requirements provide assurance as to the integrity of the information to which it relates.

Articles 8 to 11, to all intents and purposes, relate the responsibilities to be undertaken by the three parties usually involved in an electronic signature: the signatory, the CSP and the relying party.

Under Article 8(1)(a), the signatory has a duty to “*exercise reasonable care to avoid unauthorized use of its signature creation data*”. He must also notify the CSP in case of corruption of his signature creation data. An obligation imposed on the CSP as well as the signatory, concerns the exercise, throughout the life cycle of the electronic signature, of reasonable care to ensure accuracy and completeness of all material representations made by the signatory that are relevant to the certificate.

Article 9(1)(c) regulates the conduct of the CSP and imposes the necessity for a CSP to provide reasonably accessible means to ascertain from the certificate the identity of the certification service provider, that the signatory that is identified in the certificate had control of the signature creation data at the time the certificate was issued and that signature creation data were valid at or before the time the certificate was issued.

Additional obligations are contained in Article 9(11)(d) enabling the relying party to ascertain the method used to identify the signatory, any limitation on the purpose of the signature creation data or certificate and limitation on the extent of liability of the CSP, the validity of the signature creation data,

⁸¹ Article 6

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

- (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
- (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
- (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
- (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

- (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or
- (b) To adduce evidence of the non-reliability of an electronic signature.

the offer of revocation services and the means for the signatory to give notice pursuant to Article 8 in case of corruption of the signature creation data.

Article 11 imposes obligations on the conduct of the relaying party. It is up to her to ensure that she has taken all reasonable steps to verify the reliability of an electronic signature and of the certificate, observing any limitation on the certificate and checking revocation lists to make certain that the certificate has not been revoked or suspended.

These obligations, to all intents and purposes, try to distribute the burden of checking the validity of the electronic signature and the certificate so that liability for reliance on a compromised signature can be effectively attributed to the party who has not exercised reasonable care. The UNCITRAL Model Law actually promotes the use of PKIs by setting the ground for national and regional approaches to electronic signature legislation. The Model Law sets a firm base for developing countries who have yet to formulate legislation in this area and this is important for harmonization since electronic signatures are part of the international electronic commerce phenomenon. If such electronic trade is to take off then it is important that legislation in this area have the same foundations in all countries.

The 2005 APEC Telecommunications and Information Ministerial Meeting (Annex 14) took place in Lima. In its Annex D⁸² it laid down a set of guiding principles for PKI-Based Approaches to Electronic Authentication. The principles are similar to a certain extent to UNCITRAL's model law, but go much further in scope. They are intended to facilitate inter-jurisdictional acceptance of foreign certification authorities (CAs) and the development of cross-jurisdictional recognition arrangements. The Principles are also intended to help provide guidance to member economies in establishing their authentication policies and assist those with existing policies to identify and address potential deficiencies in their approach. Additionally, during the Meeting, it was stressed that while these Principles have been developed for the PKI environment, they should not be interpreted as advocating any one-technology solution over another. Rather, they focus attention on considerations in the PKI

⁸² *The development of frameworks that set out parameters for the establishment and operation of certification authorities (CAs) can facilitate cross-jurisdictional acceptance of the services they provide. Such frameworks allow for the acceptance of services originating in other jurisdictions. The establishment of legislative and legal frameworks that give legal effect to documents and signatures in electronic form produced by both domestic and foreign CAs facilitate legal predictability on a cross-jurisdictional basis. Such frameworks should not unduly require the use of particular technologies. In addition, they should allow for changing market standards, developments in existing technology and the introduction of new technology.* http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005/annex_d.html

environment in view of the predominant role played by public-key cryptography in the electronic authentication marketplace.⁸³

European Union

In a similar approach to UNCITRAL, **Directive 1999/93/EC** (Annex 15) of the European Parliament and of the Council established a Community framework for electronic signatures. The scope of the European Union Directive, as defined in its Article 1, is to effectively facilitate the use of electronic signatures and to contribute to their legal recognition. It also attempts to prioritise the use of PKIs like UNCITRAL's Model Law. Article 2 definition of electronic signature states that data in electronic form is attached to or logically associated with other electronic data and serves as a method of authentication.

The EU Directive differs from the UNCITRAL Model Law in that it includes two different types of electronic signatures: one standard and one advanced. An advanced electronic signature imposes the requirements that it be uniquely linked to the signatory, it is capable of identifying the signatory, it is created using means that the signatory can maintain under his sole control and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The EU's advanced electronic signature corresponds to that described in UNICTRAL's Model Law. The EU has set somewhat different standards for electronic signatures. The advanced electronic signature will be recognized prima facie as legally valid, whereas the electronic signature can be recognized as effective on the evidence. This distinction seems to have been put into place to strengthen authentication in electronic financial and commercial transactions as security in these domains is crucial to the development of electronic commerce. It is clear that electronic communications in the EU are as important as older forms of written communications and thus, even if such communication is not of a financial or commercial nature, it should be legally recognized where an electronic signature is applied. Such a distinction is perhaps not of immediate importance to developing nations. However, it should be noted that, although security in authentication for electronic commerce is crucial, developing countries should envisage eventual recognition of electronic signatures based on less stringent obligations for other types of electronic communications.

Article 5 of the Directive imposes on Member States the legal recognition of advanced electronic signatures which are based on a qualified certificate and which are created using a secure-signature

⁸³ THE SIXTH APEC MINISTERIAL MEETING ON THE TELECOMMUNICATIONS AND INFORMATION INDUSTRY (TELMIN6) (1-3 June, 2005 Lima, Peru)
http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005/annex_d.html

creation device.⁸⁴ It also obliges Member States to recognize the admissibility of such electronic signatures as evidence in legal proceedings. Regarding standard electronic signatures, Article 5 ensures that they are not denied legal validity on the sole ground that they are in electronic form, not based on a qualified certificate, either issued by an accredited CSP or because it was not created by a secure signature-creation device. This aims to ensure the validity of electronic signatures generally, with additional requirements to be added by Member States or to be reviewed by the Courts on a case-by-case basis. Such an approach leaves open the possibility of the creation and use of other types of electronic signatures, which are not based on the PKI system. This is important as technology is continuously evolving and future authentication methods aside from digital signatures can be granted legal validity.

Article 6 of the Directive covers the problem of liability. Here the burden is shifted onto CSPs issuing qualified certificates, making them liable for “*damages caused to any entity or legal or natural person who reasonably relies on that certificate*” regarding at the time of issuance of the certificate, accuracy of all information contained in the certificate and assurance that the signatory identified in the certificate, effectively held the signature-creation data corresponding to the signature verification data contained in the certificate.

The liability holds unless the CSP proves that it has not acted negligently. Negligent behaviour includes failure to register revocation of the certificate when there is such knowledge. The Directive additionally stipulates that CSPs may limit their liability on the use of certain certificates provided that such limitations are made known to third parties. One such limitation may concern a threshold on the value of the transaction for which the certificate may be used. The absence of such a clause would undoubtedly have a negative impact on CSPs, especially in developing countries, deterring the development and use of digital signatures. Limitations on liability can effectively help to protect nascent CSPs in developing countries, especially in the face of well-established CSPs in the US and the EU. Such an important clause could very well help foster the growth of regional CSPs in developing countries.

For example, in *Singapore*, under section 24(3) of the **Electronic Transactions (Certifications Authority) Regulations 1999** (Annex 16), all licensed certification authorities must highlight to its subscribers any limitation of their liabilities and, in particular, it must draw the subscribers' attention to

⁸⁴ ‘Qualified certificate’ means a certificate which meets the requirements laid down in Annex I and is provided by a Certification-service-provider who fulfils the requirements laid down in Annex II; ‘secure-signature-creation device’ means a signature-creation device which meets the requirements laid down in Annex III;

the implication of reliance limits on their certificates. This means that CSPs can effectively place certain limitations on liabilities, as long as they ensure that subscribers are aware of such limitations.

Four Annexes have been added to the Directive outlining requirements for qualified certificates⁸⁵, CSPs issuing qualified certificates⁸⁶, secure signature-creation devices⁸⁷ and secure signature-verification.⁸⁸ Such requirements help to establish a strong foundation for harmonization of legislation across Member States. Although put into place for better cross-border trading inside the internal market, such base could very well help to ensure international transactions in other countries not part of the EU. Similar standards would most certainly ensure supranational recognition of regional CSPs in the domain of electronic commerce, an important aspect for developing nations.

United Kingdom

In the UK, the **Electronic Communications Act 2000 (ECA)** (Annex 17) effectively implements the EU Digital Signature Directive. Three main aims of the ECA⁸⁹ are to clarify the status of electronic signatures, remove legal barriers to electronic communication and transaction and build confidence in public key cryptography. The two most relevant parts of the Act are Parts I and II.

Part I covers Cryptography Service Providers. It does not impose the registration of CSPs but does, however, highly recommend it. The ECA has, therefore, left it in the hands of the private sector to self-regulate in this area, deeming that too rigid public scrutiny and control would have a negative impact on the development of CSPs. Therefore, even if the Secretary of State were to impose onerous conditions upon cryptography service providers – for example in terms of the requirements to provide information⁹⁰ it would remain open to cryptography service providers to choose not to be part of the licensing scheme. Though they might suffer commercial loss through lack of credibility by operating outside the scheme, it would not be illegal. The self-regulatory approvals scheme will be established to ensure minimum standards of quality and service. Users will be able to check who has sent an electronic message and ensure it has not been tampered with or intercepted. If the self-regulatory scheme works, there will be no need to set up a statutory scheme. Only if self-regulation failed would the Government establish a statutory scheme, which would also still be voluntary. This part of the Bill

⁸⁵ Annex I

⁸⁶ Annex II

⁸⁷ Annex III

⁸⁸ Annex IV

⁸⁹ Electronic Law Journals – JILT 2003 – Public Key Infrastructure, Digital Signatures and Systematic Risk by Jamie Murray, Liverpool John Moores University

⁹⁰ Clause 2 (5)

will be subject to a 'Sunset Clause'. If a statutory scheme has not been set up within five years then the Government's power to set one up would lapse.⁹¹

Part II covers Facilitation of Electronic Commerce, Data Storage, etc.⁹² This makes provision for the legal recognition of electronic signatures and the process by which they may be generated, communicated or verified. It will also facilitate the use of electronic communications or electronic storage of information, as an alternative to traditional means of communication or storage.⁹³

Section 7⁹⁴ of the Act recognizes the admissibility of electronic signatures and supporting certificates, including the processes by which they are created and issued, in a court of law.

Additionally, the Act is not retroactive, which means the existing contracts, which rely on electronic signatures but are not inline with the ECA, are not void. It does not mandate the use of digital signatures or specify specific methods or processes. It aims to be technology-neutral, which will enable diverse and new technologies to be covered by the Act that may not necessarily be based upon the PKI model.

Section 8 also allows for Ministers to amend existing legislation in the face of new technological developments. This is an important allowance which certainly leaves room for flexibility and future developments, be they legal or technological.

Additionally, an amendment to the Act updated the definition of electronic communications to mean a communication transmitted⁹⁵ by means of an electronic communications network or by other means but while in an electronic form.⁹⁶

The ECA reflects the Government's compromise between the needs of the industry and those of crime prevention. It has been noted that pedophiles and terrorists, among other criminals, to effectively encrypt illegal material, have used cryptography and conspiracy plans in order to evade detection by the authorities. As encryption technologies become more and more advanced, it becomes more difficult to crack such technologies and therefore the need for key escrow has been a heated debate.

⁹¹ House of Commons Research Paper 99/92, The Electronic Communications Bill, Bill 4 of 1999-2000, 24 November 1999

⁹² Department of Trade and Industry, Information Security: Guide to the Electronic Communications Act 2000

http://www.dti.gov.uk/industry_files/pdf/622.pdf

⁹³ Explanatory Notes to Electronic Communications Act 2000 Chapter 7 <http://www.opsi.gov.uk/acts/en2000/2000en07.htm>

⁹⁴ (1) In any legal proceedings – (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and (b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.

⁹⁵ Whether from one person to another, from one device to another or from a person to a device or vice versa

⁹⁶ STATUTES ON COMPANY LAW UPDATE 4 FEBRUARY 2004 Electronic Communications Act 2000

Section 15 <http://www.oup.com/uk/booksites/content/019925947X/12886025/13539537/041eca2000.pdf>

The term “key escrow” describes a system in which the person who encrypts data has to leave the key with a third party. However, the private sector is not keen on allowing the authorities access to encrypted information. The electronic commerce market is developing quickly and the industry sector has expressed serious concerns that imposing a requirement for key escrow or third party key recovery as part of the licensing scheme would place unreasonable constraints on the development of electronic commerce in the UK. Consequently, there is a prohibition on key escrow requirements in section 13 of the Bill unfortunately to the detriment of using such means to intercept illegal and criminal electronic communications.

In the context of developing nations, it should be perhaps reconsidered, as the growing problem of illegal material, especially pedophilia, seems to stem primarily from such nations. It is an issue which has to be balanced out between the need to boost electronic commerce in a secure but unwieldy environment and the necessity of preventing a mass distribution of illegal material. The prevention of cybercrime will be discussed later on in this essay, but it is important to note that transmission of such material is also heavily dependant on cryptography and thus crime prevention should also be studied from this angle.

The **Electronic Signatures Regulations 2002** (ESR) (Annex 18) more specifically deals with electronic signatures. The implementation of the regulation follows the terms demanded of the EU Signatures Directive. Mainly, it implements the concept of advanced electronic signatures in Article 2.⁹⁷

Article 3 concerns the supervision of Certification Service Providers and the registration, recording and publishing of CSPs. In line with the EU directive, it effectively implements liability provisions on qualified CSPs (Article 4). Regulation of CSPs is being conducted in the UK through the implementation of the Tscheme. As a result of the ECA 2000, the PKI service industry united to facilitate approvals and standards for cryptographic services and to promote the development of a reliable and trustworthy infrastructure for digital signatures. The Tscheme was a response to the hands-off approach regarding Part I of the ECA, and so far has proved successful. Greater cooperation between the DTI and the industry is therefore envisaged.

⁹⁷ "Advanced electronic signature" means an electronic signature –
(a) which is uniquely linked to the signatory,
(b) which is capable of identifying the signatory
(c) which is created using means that the signatory can maintain under his sole control, and
(d) which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

The Tscheme evaluates a potential CSPs integrity by looking at different factors such as business probity and management competence, management and security policies and procedures, assurance of technical infrastructure, suitability of personnel and policies and service related policies and procedures.

The weight of the evidence is far more important in determining a person's intention, rather than the form that the signature took. The aim is to link a person to a document, and the person creating or adopting the document in electronic format must have not only the requisite intent, but also the fact that the intent must be associated to the document in some way.⁹⁸

There has been few European case law⁹⁹ regarding electronic signatures. Their validity has been accepted in most European countries without much problem. Some of the more ambiguous issues concern the admissibility of computer-generated facsimiles as electronic signature. In the UK, an obiter *dicta* in such a case affirmed that the requirements for an electronic signature were indeed fulfilled.

Europe

In France, a Decision of the Cour de Cassation¹⁰⁰, dated 30 April 2003, refers to the probative value of an electronic signature. The court in this case found that there existed a doubt on the identification of the party using the electronic signature in question and could therefore not validly be recognized as having legal effect on the contract signed between the two parties. Identification of the party is important, as outlined in the EU Directive, which states that the electronic signature must be capable of identifying the signatory.

Similarly, in Germany, the outcome of a few court cases effectively denied the proof value of unsigned emails. A case relating to the evidential value of an e-mail that was not recognized in AG Bonn (Decision of 25 October 2001). The Court decided here that hardcopies of emails do not have evidential value in court since they can be easily modified. In effect, it is not possible to verify the validity of a print out, as it is to verify its validity electronically where electronic readings would show any modification.

This is not to say that emails in electronic format cannot constitute valid proof in court. In Greece, an email message stating/confirming the recognition of a debt can be regarded as equivalent to a

⁹⁸ APPROACHES TO ELECTRONIC SIGNATURES S.C.W.MASON <http://www.pravo.by/leginform/pdf/0105/mason.pdf>

⁹⁹ Study for the European Commission- DG Information Society: The Legal and Market Aspects of Electronic Signatures by Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma & Patrick Van Eecke. Interdisciplinary Center for Law & Information Technology, Katholieke Universiteit Leuven.

¹⁰⁰ Case 00-46467

handwritten signature. One case came from a Court of First Instance in Athens, Decision 1327/2001 relating to the recognition of a debt submitted by way of an e-mail. In this case, a Czech agent concluded a service agreement with Greek travel agency by way of an exchange of e-mail correspondence. A dispute occurred, and the judge upheld the complaint of the Czech agent by recognizing the validity and the binding effect of the legal acts that were exchanged through the e-mail communications.¹⁰¹

Another form of electronic signature which has been recognized in Lithuania in a decision by the Lithuanian Supreme Court in the case *Židrūnas Šapalas v. AB "Lietuvos taupomasis bankas"*¹⁰² where the Court ruled that a PIN code for usage of payment card is equivalent to that of a hand-made signature under and for the purposes of Lithuanian contract law. In its ruling the Court emphasized that the burden to ensure reliability and security of the electronic signature system, used for payment orders, lies on the bank, and not on the user of the payment instrument. The court also stated, that in case an electronic signature (PIN code) is used for payments, *onus probandi* shall be assigned to the parties of the dispute according to the level of security of electronic signature.¹⁰³ However, a different approach was adopted in Sweden where the Howver Supreme Administrative Court¹⁰⁴ ruled that an electronic signature does not suffice for an administrative legal act to be valid. It is therefore entirely dependant on the facts of the case and the different court interpretations as to whether certain electronic signatures may be admitted as legally valid. It seems however, that a general move towards recognition of signatures under electronic format, be they PIN codes and emails, seems to be emerging, but that a hardcopy of such electronic evidence will not suffice.

United States

By contrast, the United States has approached the definition of electronic signatures by taking a functionalist approach, as set out in section 106(5) of the **Electronic Signatures in Global and National Commerce Act**¹⁰⁵ 2000 (Annex 19). This definition provides a number of elements the most important of which is that the signature is "*adopted by a person with the intent to sign the record*". This part of the definition permits any form of electronic signature to affect the function of demonstrating intent.¹⁰⁶

¹⁰¹ Supra 14

¹⁰² February 20, 2002

¹⁰³ Review of Lithuanian case law on the electronic signatures, Regija Law Firm. www.bakernet.com/ecommerce/lithuania-t7.doc

¹⁰⁴ Case number 2572-2573-2002. 18 December 2002

¹⁰⁵ 15 U.S.C. §§ 7001–7003

¹⁰⁶ Supra 14

The E-SIGN Act implements a national uniform standard for all electronic transactions that encourages the use of electronic signatures¹⁰⁷, electronic contracts and electronic records by providing legal certainty for these instruments when signatories comply with its standards.¹⁰⁸

Section 101 defines the general rule for contracts, signatures and records for which legal effect, enforceability or validity cannot be refuted solely on the fact that it is in electronic format. Similar to the UNICTRAL Model Law and the EU Directive, it goes further in view of consumer protection, requiring consumer consent to records held in electronic format¹⁰⁹ and their right to withdraw that consent at any time. Such a provision boosts consumer confidence, granting them protection against fraud and deception by those who would fail to provide consumers with adequate information. Under Section 101(c)(1)(C)(ii), consumers using electronic formats will benefit from the same protection as those using traditional paper-based formats.

The Act applies broadly to commercial, consumer, and business transactions affecting interstate or foreign commerce, and to transactions regulated by both Federal and state government. It recognizes that not only the legality of e-signatures, but also that of contracts and records will most certainly enable companies as well as consumers to transact quickly and efficiently without having to wait for paper documents to arrive, and has undoubtedly increased the volume of electronic commerce in the US. The main goal of the E-sign act is to facilitate and encourage use of such formats to build confidence in electronic commerce both for consumers and those manufacturing, producing and distributing online services and products. Consumer protection provisions of the E-sign act can prove extremely effective in countries where electronic commerce is still at its early stages, for example in developing nations, helping to promote confidence in the legal validity of such transactions and increasing security by establishing legal principles as to appropriate standards to be used regarding issues such as authentication of electronic communications with the use of electronic signatures. There is not much case law under the E-sign Act which disputes the validity of electronic signatures. Mainly litigation concerns the contract terms rather than the actual signature of the document since in the US, some contracts do not even require signatures as oral assent is often enough to make a contract binding.

¹⁰⁷ Electronic Signature: "Means an electronic sound, symbol, or process, attached to or logically associated with a contract or record and executed or adopted by a person with the intent to sign the record."

¹⁰⁸ Baker & McKenzie: E-Law Alert. USA: *ELECTRONIC SIGNATURES IN GLOBAL*

AND NATIONAL COMMERCE ACT http://www.bakernet.com/ecommerce/E-SIGN_Act.htm

¹⁰⁹ section 101.c.1

Argentina

The **Ley De Firma Digital** (Digital Signature Law) (Annex 20) was passed by Argentina in 2001. Article 3 provides for the functional equivalent of a manuscript signature, in that a digital signature is considered to be the equivalent of a manuscript signature. Other forms of electronic signature are not recognized as such unless the parties mutually recognize the form of signature that is used. If a party relies on any other form of electronic signature, it is for them to prove its validity, as provided for in article 5.¹¹⁰

A Presidential Decree covers electronic signatures and records.¹¹¹ Digital signatures, however, are limited to the national public sector. Under this Decree, the President of the Argentine Republic authorizes the use of digital signatures for two years within the sector. Additionally, the Decree provides digital signatures with the same force and effect as manual signatures for all of the "*National Public Sector which includes both centralized and decentralized administration, the autarchic entities, the state-owned companies, government partnerships, public limited companies where the government is a majority shareholder, state-owned banks and financial institutions, and any other body in which the government or its decentralized institutions have a controlling interest* (5)."¹¹² This Decree has helped to establish confidence in electronic signatures by the fact that it is being validated by the government ensures public confidence that their use will be legally recognized and enforceable in a court of law.

Another Presidential Decree¹¹³ was passed on August 13, 2001 allowing for purchasing by digital means and digital signatures. This applies to private sector as well as public, ensuring that electronic commerce is fully licensed and legally valid, and therefore subject to the same standards as traditional commerce. This two-step approach has effectively ensured confidence in electronic trading along with the use of electronic signatures to validate such trading.

Concerning CSPs, a new regulation¹¹⁴ regarding the licensing of Certification Authority within the Argentine Government was enacted on December 30, 1998 and limited to the national public sector. This is a start for ensuring functionality and effectiveness of CSPs, testing its success and remedying potential flaws and security issues before applying it to the private sector. This cautious approach will ensure eventual credibility and validity in CSPs once they are used in the private sector.

¹¹⁰ APPROACHES TO ELECTRONIC SIGNATURES S.C.W.MASON <http://www.pravo.by/leginform/pdf/0105/mason.pdf>

¹¹¹ Signed by President of Argentina April 16, 1998, No. 427/98

¹¹² <http://www.american.edu/carmel/gg7870a/Transborder.htm> IT Landscape in Argentina: Transborder Data Flows, American University of Washington D.C.

¹¹³ 1023/01

¹¹⁴ Resolution 212/98

Authentication as the provision of proof that the claimed identity of an entity is true undoubtedly helps to ensure security when dealing in electronic commerce. This includes authentication of devices, services and applications as well as identity. It also permits non-repudiation, which is the ability to prevent users from denying later that they undertook a particular transaction. This certainly helps to undermine fraud and deception. Assurance of peer entity and data origin can be guaranteed by encryption methods. It is clear that a move towards a bias for public key infrastructure has developed and this can be seen in UNCITRAL's Model Law and in the EU Directive. However, the possibilities that new technologies may develop that are more secure than PKI should always be envisaged when drafting legislation. A look at the US E-sign Act and the UK's Electronic Signatures Regulation place more emphasis on the protection granted to consumers and to the weight of the evidence rather than the form of the signature. A more technologically neutral approach, including provisions sustaining the PKI model, but not excluding the possibility of embracing future technologies, would be ideal for countries wishing to develop a legal base for security in electronic commerce.

ACCESS CONTROL & COMMUNICATION SECURITY

Access control can be defined as protection against unauthorized use of network resources. This can be implemented by passwords, physical devices such as biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, audit trails, and monitoring by automated systems and people. The importance of having a safeguard in legislation regarding access is primary. Control of access to computer systems and networks is vital, as it appears that unauthorized access is the main portal to computer-related crimes.¹¹⁵ Penal provisions regarding illegal access to such systems can effectively deter computer crime.

Communication security ensures that information flows only between the authorized end points in that the information is not diverted or intercepted as it flows between these endpoints. This ensures data integrity and the prevention and detection of any illegal interception and modification.

Council of Europe

The Council of Europe **Convention on Cybercrime in 2001** (Annex 21) was the first international initiative on computer crime. It has been signed by 37 States and entered into force in July 2004. It has currently been ratified by 10 States. Chapter II of the Convention includes measures to be taken at

¹¹⁵ Cole Durham, Brigham Young University, Utah, USA

the national level and covers details of offences against the confidentiality, integrity and availability of computer systems and data. This includes unauthorised access offences.

Article 2¹¹⁶ makes illegal access an offence. Illegal or unauthorized access to computer systems and data is the basic cybercrime. Data designates information for both people and computers. Illegal access can be also defined as hacking, cracking and computer trespass. The requirement of intentionally securing access to data establishes such access as an offence, even when no access is achieved. These access provisions can be considered as trespass provisions. One important aspect of access is the fact that the information need not be downloaded. The fact that it can be read means it is accessible and thus constitutes an offence.

The Convention uses technologically neutral language in order to anticipate future technological advances. For criminal liability to apply, the offences must be committed intentionally, either willfully or knowingly, and must be committed without right with the view not to criminalize legitimate activities inherent to the design of networks and common commercial practices.¹¹⁷

Article 3 covers illegal interception.¹¹⁸ It effectively criminalizes interception of privately transmitted data and information, if such interception is committed intentionally and without right. The Article allows for inclusion of a dishonest intent in the commission of the activity, but the Article does not however mandate this. It is clear that the broad language of the Convention leaves it open to signatory states to decide how they want to implement these clauses into their national legislation, without constraining them with too much detail.

The essence of these two articles criminalizes illegal access and interception. Such conduct however is not meant to deter legitimate computer security, research and education practices. Consequently, it is important to note that such access and interception is only illegal when committed ‘without right’. Article 6 effectively criminalizes the trafficking and possession of hacker tools only where such conduct is intentional, without right and most importantly, done with the intent to commit an offence. The Convention does not in itself lay down provisions for exemptions from these articles. It is up to

¹¹⁶ *each party is to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

¹¹⁷ Harmonizing National Legal Approaches on Cybercrime by Judge Stein Schjolberg & Amanda M. Hubbard, ITU WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June – 1 July 2005

¹¹⁸ *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*

the signatory countries to make exemptions in their domestic laws. This is mainly because very different laws exist in all countries and it would prove impossible for the Convention to elaborate detailed legislation which might prove conflicting with certain countries existing legislation.

The Convention helps to foster international cooperation by criminalizing the basic cybercrimes. The ideal is that all signatory states have the same legislative foundation, regardless of further domestic laws in this area, which will enable prosecution of crimes committed in one country but which have an effect on several different countries.

Article 13 stipulates that members to the convention must take necessary measures to ensure that criminal offences are established in accordance with Articles 2 to 11, which are punishable by effective, proportionate and dissuasive sanctions, including prison terms.

Under Article 14, search and seizure of computer data is allowed for collection of evidence regarding the alleged or actual commission of an offence. Under Article 19, jurisdiction is dealt with but has very far-reaching elements. Under 19(1)e, any offence relating to Articles 2 - 11 is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. The Article seems to be an overreaction to the global nature of the Internet. It creates criminal penalties for actions of nationals who have no connection with the country other than holding its citizenship. It also creates grossly unfair situations. A US citizen who has lived for 20 years in another country who is accused of violating copyright law could be charged in an American court for something that has no connection to the US. It would also appear to be an attack on non-affiliated jurisdictions such as Sealand.¹¹⁹

European Union

The EU wished to further legislation in this domain and thus formed a proposal for a **Council Framework Decision on attacks against information systems** 2002 (Annex 22).¹²⁰ On 24 February 2005 the JHA Council finally adopted the framework decision on attacks against information systems. The decision harmonizes legislation in the EU for any offence committed against a computer

¹¹⁹ A Draft Commentary on the Council of Europe's Convention on Cybercrime, October 2000
http://privacy.openflows.org/pdf/coe_analysis.pdf

¹²⁰ published April 19, 2002.

infrastructure with the intention of destroying, modifying or altering the information stored on computers or networks of computers. The term information systems is actually used in a very broad sense, perhaps something the Convention on Cybercrime lacks. The definition is meant to include not only networks of computers, but stand-alone computers as well, personal digital organizers, mobile telephones, intranets, extranets and other servers and infrastructures of the Internet. The term information systems is used in order to incorporate future technological developments in this definition. The two key definitions in the decision are illegal access to information systems and illegal interference with the system. In both cases, intent has to be proven to rule out gross negligence or recklessness, and legitimate access and interception. The decision covers not only offences affecting the Member States but also offences committed in their territory against systems located in the territory of third countries.¹²¹

Article 2 concerns illegal access to information systems¹²². This includes the notion of hacking, the unauthorized access to computers and networks, undertaken in a variety of ways, from physical attacks on networks or through the use of inside information. Cracking, on the other hand, is often committed with a malicious intent. Hackers sometimes illegally access systems to expose security flaws in order to help build better and tighter security systems. Often a positive aspect, although blatantly illegal, it might not be ideal to severely punish such activities. The main aim of the Article is to criminalize the offence to the extent that such access was committed with intent to cause damage to a natural or legal person and with the intent to result in an economic benefit. Furthermore, there is no requirement that security measures must have been overcome for the offence to be committed since many private individuals do not protect their systems in any way, and including such a requirement would effectively exclude them from protection against unauthorized access.

The approximation of substantive laws ensures that a minimum level protection for victims of cybercrime will help to meet the requirements that an activity is classed as an offence in both countries before mutual legal assistance can be provided to assist in investigating and prosecuting the crime. Although the European Union is very close to achieving this, the deterrence of computer related crime will only work effectively if all countries make a global effort to harmonize their national laws.

In the EU, there is a general principle of confidentiality of communications, which means that any interception is illegal unless specifically authorized by law. This follows from Article 8 of the

¹²¹ Council adopts decision on attacks against information systems 10 March, 2005 Digital Civil Rights in Europe [EDRI-gram - Number 3.5](http://www.edri.org/edriagram/number3.5/attacks) <http://www.edri.org/edriagram/number3.5/attacks>

¹²² access to the system is subject to specific protection measures; access is obtained with the intent to cause damage or obtain economic benefit.

European Convention on Human Rights, the right to respect for private and family life. This fundamental right to privacy effectively limits interception of communication to criminal investigations, ensuring that the individual is informed of any interception of communication.

United Kingdom

Similar to the EU Directive articles against unauthorized intrusion, the UK's **Computer Misuse Act 1990** (Annex 23) serves to penalize individuals hacking and related computer activities that access systems which they have no authorization to access. Section 1(2) does not require any malicious intention on behalf of the perpetrator. However, the perpetrator in so accessing computer material knows that such access is unauthorized. This is what characterizes the criminal element of such access, consequently determined by the *mens rea* of the perpetrator at the time of access.

The Act covers unauthorized access to computer material.¹²³ The two main requirements to establishing an unauthorized access offence are knowledge and intention. The perpetrator must have intended to access a specified system and have the requisite knowledge that such access was unauthorized. The element of intention does not specifically refer to either a malicious or benevolent intention, and as such, has a broad application. Knowledge however is a more difficult element to prove. Suspicion that such access is unauthorized is unlikely to succeed in a court of law as it falls short of actual knowledge. One of the more difficult problems is when passwords to certain systems are given by a friend or readily available for download on the Internet. A password granted by a colleague does not necessarily determine actual knowledge that use of it to access a system is unauthorized. Additionally, a difficult issue is when a user clearly displays that access to a particular system is unauthorized but does not add any security measures to prevent illegal access. This is a difficult point and the lack of case law in this area leaves open speculation about the direction in which jurisprudence will go.

There exist a few cases nonetheless in this area. In *Denco v. Joinson*,¹²⁴ the appellant had been granted limited access to the computer system in connection with his employment as a metal worker but allegedly sought to access information relating to the firm's customers, information which fell outside the scope of his access rights. The appellant, who sued for unfair dismissal, had made use of an ID and password allocated to another employer. The computer culture existing within the workplace may be a

¹²³ A person is guilty of an offense if-

(a) he causes a computer to perform any function with the intent to secure access to any program or data held in any computer,

(b) the access he intends to secure is unauthorized, and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

¹²⁴ Employment Appeal Tribunal 14 November [1991] 1 WLR 330

matter of some importance in this respect. It was reported that in the initial stages of computerization, management encouraged employees to make use of the computer even though this was not required for the performance of their duties. In such a climate, it might be difficult to establish the requisite knowledge.¹²⁵

In *R v Cropp*¹²⁶, the court confirmed that Section 1 of the Act applies to insiders who access computers. Similarly, in *R v. Bignall (16 May 1997)* the Computer Misuse Act 1990 only covers unauthorized access to a computer or to data held on it, and not mere access by authorized users of the computer and data for an unauthorized purpose. Where an employer places a restriction on access to data held on a computer in circumstances where such access is required for the purposes of an employee's work, if the employee willfully disregards the restriction as to purpose, there is no ground for action under the Act.¹²⁷

In *Regina v Bow Street Magistrates Court Ex parte Allison QBD (Times 2nd of June 1998)*¹²⁸, an American employee of a credit card company was accused of using her privileged access to the computer systems to milk various credit accounts. In addition, it is alleged, she arranged to supply information to Mr. Allison in the UK who in turn used that information to defeat the ATM system by the use of the pin number details revealed to him. The case does not discuss the guilt or innocence of Mr. Allison, but the question of whether individuals committing offences under the Computer Misuse Act were extraditable to the USA in the absence of particular reference to that Act in the various regulations under the Extradition Acts. It was held that offences under Section 2 and 3 of the Computer Misuse Act, being offences punishable with more than one year's imprisonment, were so extraditable. Another, possibly more interesting, question discussed was the meaning of 'authorization' under the Computer Misuse Act. The case suggested that within an employment situation and without explicit company policies to cover the situation, an employee who actually has access to computers as part of his work will have the appropriate authority under the Act to access data.

Concerning unlawful interception, the **Regulation of Investigatory Powers Act 2000 (RIPA)** (Annex 24) creates the criminal offence in relation to the unauthorized interception of communications, both public and private telecommunication systems, thus addressing itself to Internet Service Providers as

¹²⁵ Electronic Frontier Foundation, *Crime and the Computer: The Unauthorized Access Offence*
<http://www.strath.ac.uk/Departments/Law/dept/diglib/book/criminal/crim15.html>

¹²⁶ [Attorney-General's Reference (No. 1 of 1991)] [1992] 3 WLR 432]

¹²⁷ The Journal Information Systems Committee, Senior Management Briefing Paper: *New Developments in UK Law* April 2000 www.jisc.ac.uk

¹²⁸ Law-bytes, *Computer Misuse and Extradition*, Wrigley Claydon - Solicitors Oldham and Todmorden,
<http://www.swarb.co.uk/lawb/cpucmaExtradition.shtml>

well as telephone service providers under section 1.1 of chapter I.¹²⁹ RIPA makes it a criminal offence to “*intentionally and without lawful authority*” intercept any communication in the course of transmission, unless there is implied or express permission to intercept such communication by the sender or by a person who has a right of control over a private telecommunication system as stipulated under section 1.6 (a) and (b). Exceptions in the Act allow for persons running a telecommunication service for purposes connected with the operation and running of the service to intercept communication in order for example, to redirect misaddressed emails or to filter out virus-infected mails and SPAM.¹³⁰

Communications may be monitored and recorded however in the interest of national security, for the prevention of crime, for the detection of unauthorized use of telecommunication systems and to secure an effective system operation. These exceptions are nonetheless subject to the requirement of using all reasonable efforts to inform the sender/receiver that his communications are monitored and recorded under section 3.1(a) and (b). Such notice can be inserted, for example, in the terms of a contract between an employer and employee. Concerning interception by public authorities, a lawful authority requirement for interception warrants is needed for it to be legitimate (section 5). The grant of an interception warrant is subject to certain conditions as laid out in section 5.3 (a), (b), (c) and (d)) regarding national security, economic interests of the country, the prevention of serious crime and in the context of an international mutual assistance provision.

Regarding the Act, the courts have not yet established case law in this area. It is however clear, that all institutions, be they governmental, educational, social or private, may not arbitrarily intercept communications without the express consent of both the sender and the recipient.

¹²⁹ 1. - (1) *It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of-*

(a) a public postal service; or

(b) a public telecommunication system.

(2) It shall be an offence for a person-

(a) intentionally and without lawful authority, and

(b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection, to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system. (3) *Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either-*

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system.

¹³⁰ Senior Management Briefing Paper 14: The Regulation of Investigatory Powers (RIP) Act 2000: Email and Telephone Monitoring, JISC Published 2 Jul 2001 http://www.jisc.ac.uk/index.cfm?name=pub_smbp_ripa

United States

Additional case law in the US¹³¹ can prove helpful in determining the direction of jurisprudence in this field. In *Briggs v. State of Maryland*¹³², the Court held that the statute of the state of Maryland that criminalizes unauthorized access to computers "*was intended to prohibit use of computers by those not authorized to do so in the first place, and may not be used to criminalize the activities of employees who use employers' computer systems beyond the scope of their authority to do so*". In contrast to the UK case of *Denco*, it seems here that employers within a company, although not specifically granted access, cannot be prosecuted for an unauthorized access offence.

Similarly, in *Scott Moulton and Network Installation Computer Services, Inc. v. VC3*¹³³, the Court held that the plaintiff's act of conducting an unauthorized port scan and throughput test of defendant's servers does not constitute a violation of either the Georgia Computer Systems Protection Act or the Computer Fraud and Abuse Act. Port scans are a difficult notion to grasp, since they are the pathway to informing the user of potential security vulnerabilities and potentially enabling him to access vulnerable computers. However, the act of port scanning is not in itself an unlawful activity, though it may lead to an offence, as the ownership of a crowbar is not illegal in itself, since many other legitimate uses can be found for it.

Australia

Australian case law¹³⁴ however has taken a different approach regarding employers. In *Regan Gerard Gilmour v. Director Of Public Prosecutions*¹³⁵, a public servant working for the Australian Taxation Office, in the Relief Section, was not permitted by his employer to enter a relief code "43" in 19 different cases where no grant of relief had been made and the accused knew this to be the case. However, in all the 19 cases, the accused inserted data, relief code "43", in the computer indicating that relief had been granted. The computer received this data in each case. There was no financial gain to the accused in taking this course. He did so because of a desire to expedite the process, a heavy workload and concern about suggested inconsistencies in determinations of applications for relief. The Court was required to determine whether the accused had "authority" to insert data in a Commonwealth

¹³¹ Asian School of Cyberlaws, Cyber Crime Cases, Emerging Jurisprudence, http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm

¹³² 348 Md. 470 (1998) [USA]

¹³³ Civ. Act. No. 1:00-CV-434-TWT (N.D. Ga. November 6, 2000) [USA]

¹³⁴ *Ibid*

¹³⁵ (Commonwealth) No. 60488/95 In The Supreme Court Of New South Wales [Australia]

computer for the purpose of section 76C¹³⁶ of the **Crimes Act 1914** when the computer would physically accept his insertion of data, but “the accused was not permitted by his employer to insert the relevant data, relief code "43", in the computer without specific permission given by the employer prior to the insertion and such permission was not given in these cases". The Court held that a person commits an offence under this section if he lacks the authority to insert the particular information into a computer, notwithstanding that he has general authority to insert other information into such computer. The Court further held that an entry intentionally made without lawful excuse and known to be false is made without lawful authority.

In the case of *Director of Public Prosecutions v Murdoch*¹³⁷, the court held that section 76 C of the Crimes Act 1914 does not distinguish between hackers and persons who are authorized to enter the computer system. The section looks to whether the particular access to the computer system was with or without lawful authority. The Court stated that where the question is whether the access was with permission, it needed to identify whether such access was within the scope of the granted permission. If the permission were not subject to some express or implied limitation, then the access would be lawfully justified. However, if the permission were subject to a legitimate limitation, then the entry would be without lawful authority to do so.

The Court also held that in the case of an employee the question would be whether that employee was allowed authorized access. If he had a general and unlimited permission to access the system, then no offence has been committed. On the other hand, if limits on the permission given to him to access that system exist, he must seek permission whether access he is seeking is within the scope of that permission. If so, then no offence can be committed; if not, then he has accessed the system without lawful authority to do so. This is a very different view to that entertained in the US courts and perhaps demonstrates a more thorough understanding of access to a system by looking at the lawful authority element. This is perhaps a safer approach for developing countries in order to avoid widespread corruption inside companies by employees. It is recommended that authorized access should be checked with lawful authority.

¹³⁶ As per section 76C of the Crimes Act 1914, "A person who intentionally and without authority or lawful excuse: (a) destroys, erases or alters data (Data" is defined by section 76A as including information, a computer program or part of a computer program) stored in, or inserts data into, a Commonwealth computer..... is guilty of an offence".

¹³⁷ (1993) 1 VR 406 [Australia]

3. SECURITY OF INFORMATION INFRASTRUCTURE

INTEGRITY OF DATA: DATA SECURITY, PRIVACY & CONFIDENTIALITY

Data integrity is defined to mean data that has not been altered in an unauthorized manner. This includes both privacy and confidentiality in its scope. Privacy is the right of individuals to control or influence what information related to them may be disclosed. Confidentiality relates to the protection against unauthorized disclosure of data content.

Privacy is one of the fundamental tenets of democracy and it has been entrenched within the international human rights framework from the Bill of the Rights to the many regional instruments. The laws relating to privacy, however, are peculiar. For example, within the European Convention on Human Rights (ECHR), there is a provision for a limited protection of family and private life. The European Court of Human Rights has been very meticulous in interpreting this within stringent lines and has often afforded Member States a wide margin of appreciation. The ECHR nevertheless permits the State to derogate from the right of private and family in certain cases.

Article 8 of the ECHR covers the right of respect for private and family life, the home and the individual's correspondence.¹³⁸ The Internet, by enabling the delivery of a wide range of electronic communications services over a common, global infrastructure, opens new opportunities for users but also creates new risks for their personal data and privacy. It is therefore important to protect data with regards to the increasing capacity for automated storage and processing relating to subscribers and users of electronic communication services. Legal and regulatory, as well as technical, provisions must be ensured concerning the protection of personal data and privacy must be enacted in order to

¹³⁸ There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

safeguard the legitimate interests of data subjects. Consequently, maximum harmonization is necessary in such laws if the development of new electronic communication services and networks is to be assured.

Council of Europe

The Council of Europe's **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (Annex 25) was signed in Strasbourg on January 28, 1981. Data is information regarding persons which enables their identification as an individual. The Convention looks to the protection of information in processing and filing operations such as data storage, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination by automated means. The purpose of the Convention is to guarantee respect for people's fundamental rights and freedoms, particularly the right to privacy.

Article 5 of the Convention looks to the quality of the data and the acquisition and processing of any data is to be done fairly and lawfully and requires that any storage must only be enabled for specified and legitimate purposes, and that this should be adequate, relevant and not excessive in relation to the purposes for which they are stored. Additionally, the data stored must be accurate and updated where necessary. Such information should not be kept, however, for longer than the purposes for which the data was initially stored. Once such purpose has become obsolete, the data should be erased.

Under Article 6, sensitive data revealing information on race, political, religious or other beliefs, health and sexual data may not be processed automatically unless appropriate safeguards exist in the country where such data is being held. This added precaution is needed because of the sensitive nature of such data.

Article 7 concerns data security in an electronic environment. Security must be imperatively assured as such data can be easily accessed and corrupted as opposed to paper counterparts which can be securely locked up in a safe. If unauthorized users can access such data, the facility with which multiple copies can be made and transmitted would entail a serious breach of privacy and confidentiality. Therefore, it is important that appropriate security measures be put into place to safeguard against unauthorized access and use.

Additional safeguards have been added in Article 8 to ensure that the data subject is able to ascertain who the holder of data concerning her is, the main purposes of holding such data, as well as the identity and habitual residence or principal place of business of the controller of the file. The subject is also allowed to have such data communicated to her in an intelligible form if she so wishes. The subject is

furthermore entitled to request rectification or erasure such data if it has been processed in a way that does not accord with domestic law and to obtain a remedy if a request for confirmation, communication, rectification or erasure of data if, as the case may be, there is error regarding her data, or if the subject just wishes to have it communicated to her. Such a provision allows for the data subject not only to be made aware of data held about her, but also enables her to rectify it in case of error, or erasure of the data in the case where the initial purpose of storage has become out of date.

The only exceptions and restrictions permitting derogation from the previous articles concern the protection, where necessary, of State security, public safety, the monetary interests of the State or the suppression of criminal offences and for the protection of the data subject or the rights and freedoms of others. These derogations are stipulated in Article 9 of the Convention and are applied after a balance of interests has been weighed between the necessity to protect the privacy of the data subject and the other factors listed in the Article.

With respect to transborder data flows, Article 12 stipulates that no country is to prohibit such flow for the sole purposes of protection of privacy. However, it may prohibit it on the grounds that the receiving country does not have adequate domestic legislation guaranteeing the safeguards in the Convention or it may prohibit transfers through to a third State with adequate protection but where the final destination is in a State where such safeguards as found in Articles 5 to 9 in the Convention are not guaranteed.

If developing countries want to participate in e-commerce globally that their national legislation ensures the same level of protection granted by other countries regarding storage and processing of personal data. This is imperative if these countries want to commerce with European Union countries, which have very strong data protection laws. Trading with the EU might prove difficult if an inferior level than that found in the EU subsists, as the Community countries will not allow transfer data if protection in third countries is found to be wanting.

United Nations

The **UN Guidelines concerning computerised personal data files** (Annex 26) list a few principles for the elaboration of legislation in States. Initiatives are, however, left to the States regarding implementation of such legislation, although they should follow the principles laid down in the Guidelines as closely as possible. The first principle ensures that data collection is done in a lawful and fair manner in compliance with the UN Charter. The second principle of accuracy guarantees that the

collector of data undertakes regular checks on the data to make certain it is accurate and kept up to date.

The principle of purpose-specification identifies the purpose which a data file is to serve and ensures that it is used legitimately and brought to the attention of the data subject. This guarantees that the data collected remains relevant and adequate to the purposes specified, that the consent of the subject data is assured with regards to the use of her data outside the purposes for which it was initially collected and that the period of storage of the data does not exceed the date limit of the purpose.

The principle of interested persons access reflects Article 8 of the Council of Europe Convention regarding communication to the subject of data held and to ensure that such data is used legitimately. The principles of non-discrimination, power to make exceptions, security and transborder data flows all closely reflect those already outlined in the Council's Convention. Similar procedures can also be found in the OECD's privacy guidelines.

European Union

The EU has effectively put into place a directive in view of data security, [Directive 95/46/EC](#) (Annex 27) of the European Parliament and of the Council of 24 October 1995 on the **protection of individuals with regard to the processing of personal data and on the free movement of such data**. The main objective of the Directive, as outlined in Article 1, is to protect fundamental rights and freedoms of natural persons, and in particular the right to privacy with respect to the processing of personal data and to ensure the free flow of data within the internal market. The Directive concerns processing of personal data wholly or partly achieved by automatic means and by means other than automatic which forms part of a filing system. The Directive follows the same general principles as the Council of Europe's Convention. However, it goes into much more detail and is more specific.

Section I of the Directive covers principles relating to data quality. Article 6 stipulates that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. The data collected must also be adequate, relevant and not excessive in relation to the purpose and accurate, and where necessary, kept up to date. Section II of the Directive covers the criteria for making data processing legitimate. Under Article 7, the data subject must have given her consent. Additional requirements are listed, including for the performance of a contract, for compliance with legal obligations, for the protection of the data subject's vital interests, for the performance of tasks carried out in the public interest and for the carrying out of legitimate purposes by the controller of the data.

Special categories of data are added in Section III under Article 8, similar to those found in the Convention regarding ethnic, racial, political, trade union, health and sexual data. Derogations have been included, however, covering explicit consent of the data subject along with obligations under employment law, protection of vital interests of the data subject, the public interest, the exercise of legal functions and for criminal purposes.

Section IV (Article 10) covers the information to be given to the data subject if she so requires it, and Section V (Article 12) allows for the data subject's right of access to data held on her. Under Section VII, Article 14, the data subject has a right to object to data relating to her being processed for purposes of direct marketing or for the disclosure to third parties for the first time.

Of more relevance to the subject is Section VIII on confidentiality and security of processing. Article 16 ensures the confidentiality of the processing of personal data and Article 17 stipulates that Member States need to implement appropriate technical and organizational measures to protect personal data against accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves transmission of data over a network. The processor must provide for sufficient guarantees of technical security measures depending on the risk level of processing and the nature of the data to be protected. Controllers must therefore have regard to the state of technology and the cost of implementing security measures, balancing this with the risks involved when processing data. It is thereafter up to Member States to decide specific levels of security to be adopted. One example would be the suitability of the use of emails to transmit confidential information and perhaps the imposition of the use of encryption technology to ensure confidentiality and integrity of the data.

The data protection Directive has two main aims, the protection of individual's privacy rights and the assurance of the free flow of personal data between Member States. However, when dealing with third countries, these two aims are not always compatible. It is nonetheless important that such protection be afforded uniformly throughout countries wishing to be networked so as to allow the uninhibited flow of information between them.¹³⁹

Directive 2002/58/EC (Annex 28) of the European Parliament and of the Council concerns the processing of personal data and the protection of privacy in the electronic communications sector. This Directive complements Directive 95/46 on the protection of the processing of personal data, but applies more specifically to the electronic communications sector. It replaces Directive 97/66/EC which outlined specific rules for the telecommunications sector. The new Directive, however, has been

¹³⁹ See also Regulation 45/2001/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

adapted to developments in the markets and technologies for electronic communications services for users of such publicly available services, regardless of the technologies used. The new Directive takes into account new advanced digital technologies such as digital mobile networks and the Internet.

Article 4 of the Directive covers security, stating that the provider of a publicly available electronic communications service (hereinafter 'e-service provider') must take appropriate technical and organizational measures to safeguard security of its services. The level of security should be proportionate to the risk presented. In case of a risk of breach of security of the network, the e-service provider is under a duty to inform the subscribers of the risk and of possible remedies in case of the risk outweighing the scope of measures available to the provider, along with an indication of the possible costs involved.

Article 5 imposes on Member States the requirement to elaborate national legislation protecting the confidentiality of communications and the related traffic data. A prohibition on listening, tapping, storage and other kinds of interception or surveillance of communications, without the consent of the user concerned is imposed. Derogations to this Article are applied from Directive 95/46/EC, in the case of safeguarding national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications system.¹⁴⁰ Article 5 does not, however, prevent the storage of communications where it is necessary for further conveyance and transmission.

Other exceptions to this Article apply when such storage is in the course of a lawful business practice and when the subscriber has been fully informed and she has given her full consent in accordance with Directive 95/46.

Article 6 concerns traffic data that must be erased or made anonymous when it is no longer needed for the purposes of transmission of a communication. The data may be kept for the requirements of subscriber billing and interconnection payments. Concerning marketing purposes, the traffic data may only be retained if the subscriber has given her consent. Subscribers should be given the option of withdrawing their consent at any time. The e-service provider must also inform the subscriber, prior to obtaining consent, the duration of the use and the types of traffic data that will be used for marketing purposes. Finally, processing of such data must only be handled by the competent persons acting under the authority of the e-service provider.

¹⁴⁰ Article 15 of Directive 2002/58

Article 9 concerns location data and is subject to the same conditions as traffic data concerning consent of the data subject. Such data must be rendered anonymous or deleted once it has fulfilled its initial purposes unless the consent of the subject is given.

Similarly, concerning directories of subscribers, under Article 12, Member States are obliged to ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services. Consent needs to be sought concerning the type of data displayed in the directory and all information regarding such data needs to be given to the subscriber. Article 13 deals with unsolicited communications and provides that they may only be allowed to subscribers who have given their prior consent.

The European Court of Justice has already held hearings concerning data protection against the disclosure of the income of employees. In the case of *Rechnungshof*¹⁴¹ on the interpretation of Directive 95/46, the defendants did not communicate the data on the income of the employees in question in anonymised form. The Court considered that comprehensive information for the public as intended by the national legislature has to be regarded as interference with private life which can be justified under Article 8(2) of the ECHR only if that information contributes to the economic well-being of a country. An interference with fundamental rights cannot be justified by the existence of a mere public interest in information. The Court stated that such publication of personal data constituted a disproportionate interference with private life.

¹⁴¹ C-465/00, 20 May 2003

The Directive prudently only permits data collection and retention measures where necessary, appropriate and proportionate within a democratic society. Further, the idea of a blanket data retention measure was clearly rejected.¹⁴² Data retention effectively interferes with the ECHR's right to respect for private life. Indiscriminate retention of data is not in accordance with law nor with other protected areas such as confidential attorney-client relationship for example. The dangers of retaining a massive database include potential abuse of such information not only by private actors like hackers, but also by state authorities and raise concerns about the misuse of sensitive personal information. Such dangers could very well undermine public confidence in electronic communications systems. Recital 5 of the Directive recognizes that the successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk. Finally, indiscriminate data retention would inevitably raise prices of public communications systems by imposing retention on a massive scale. This would, without doubt, be a charge borne by the end user.

Consequently, data retention is not such a good idea for developing nations as not only does it severely constrain individuals right to privacy, but creates additional problems such as increased costs and potential exploitation of personal data which could inhibit use and development of e-service providers. Limitations to those cases where there are valid reasons for retaining data as outlined in the Directive suffice to ensure adequate safeguards on privacy and confidentiality without inhibiting the development of communications services.

United Kingdom

The UK **Data Protection Act 1998** (Annex 29) implements data protection provisions consistent with the EU Directives discussed above. The eight principles, which constitute the substantive provisions of the Data Protection Act, are quite similar to the core provisions found in Directive 95/46/EC.

According to the first principle, personal data must be processed *lawfully and fairly*.

The data should not be processed in a manner that is incompatible with the purpose for which the data is being processed. This means that the personal data processed must be *relevant, adequate and not excessive* in relation to the purpose. The data also must be kept accurate and up to date. The personal data should additionally not be kept for longer than it is necessary to fulfill the purpose of processing the data. The data must be processed in accordance with the rights of the data subject.

¹⁴² Privacy International, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, 10th October 2003, Prepared by Covington & Burling, http://www.privacyinternational.org/issues/terrorism/rpt/data_retention_memo.pdf

With regard to security measures, *appropriate technical and organizational measures* are to be taken against unauthorised and unlawful processing and against accidental loss, destruction and damage to the data. Finally, the last principle deals with cross-border flows and states that personal data is not be transferred to a third country which does not ensure an adequate level of protection to the rights and freedoms of the data subject in relation to the processing of personal data.

The judgment of the Court of Appeal in *Durant v Financial Services Authority*,¹⁴³ however, stressed that the Data Protection Act was not there to help individuals with matters other than protecting their privacy. In this case, Mr. Durant was litigating with the FSA and Barclays Bank and needed the information for this case. The court was clear about the purpose of an access request: to enable an individual to check whether processing of personal data unlawfully infringes his privacy and, if so, to take steps to protect it. The right does not automatically give rise to the right to have that information about matters in which the individual may be involved.

According to section 4 of the Act, the data controller has a duty to comply with the Data Protection principles in relation to all personal data of which he is the controller. This means, for example, that company directors need to ensure that up-to-date technology is in place and that additional security measures are added on a regular basis. The liability holds not only directors but also for employees who have access to personal data. This means that an employee policy must be put in place and effectively policed.¹⁴⁴ In the case of *Academy Credit Limited*¹⁴⁵, the directors were found guilty of illegally trying to procure information in an attempt to sell that information to interested parties. The investigation and prosecution of Academy Credit Services Limited and its directors was a direct result of the Inland Revenue notifying the Information Commissioner that it had been targeted by the company in attempts to procure information.¹⁴⁶ The directors in this case were held criminally and personally liable for acts committed by the company.

As well as criminal liability, the DPA holds civil liability. This can occur in the case of an insecure website where companies have problems with online security. Consequently, the importance of being technologically capable of adequately protecting personal data within the constraints of the DPA is essential. This includes keeping employees in companies aware of the information being held and the limitations on the use of that information.

¹⁴³ [2003] EWCA Civ 1746

¹⁴⁴ Privacy – The Voice of Business, Jonathan Armstrong, “Personal Data Protection – Policy and Practice in EU Accession and New Member States”, <http://privacy.gateway.bg/htmls/en/home.htm>

¹⁴⁵ Chichester Crown Court on 18 December 2001

¹⁴⁶ Oscura News: Directors found guilty under DPA 1998 21 December 2001
http://www.oscura.co.uk/show_news.asp?news_id=9

The UK **Privacy and Electronic Communications Regulations** (Annex 30) effectively implement EU Directive the Telecommunications Data Protection Directive 97/66/EC, which was replaced by Directive 2002/58/EC. The security provisions in Article 4 are implemented in Regulation 4 of the Privacy Regulations. These largely reflect the wording of current requirements except that they now include the wording used in Recital 20 on the provision of information free except for a nominal charge.

The confidentiality requirements were mostly implemented in the UK by the **Regulation of Investigatory Powers Act 2000** (RIPA), which prohibits interception and recording of communications (including e-mail) without consent, except as authorised for national security and law enforcement purposes, or essential business purposes. RIPA sets out the terms on which public authorities may access communications and traffic data. The terms on which businesses may intercept and record communications without consent are set out under the Telecommunications Lawful Business Practice Interception of Communications Regulations 2000 secondary legislation under RIPA.

Europe

In France, the French Data Protection Authority, Commission Nationale de L'Informatique et des Libertés ("CNIL"), has ruled that an email service provided by Rampell Software, a Florida-based company, is illegal, as it breaches French data protection law.¹⁴⁷ Subscribers to the service, called 'Did They Read It?' are able to track all emails that they send without the recipient's knowledge. The software informs subscribers when recipients have received their email, what time they opened it and for how long it remained open on their screen. It also provides further information such as how many times the email was viewed, the type of operating system used by the recipient, who the email was forwarded to, and whether the secondary recipients opened the message.

Under European Data Privacy legislation, such collection and transmission of data is unlawful. Under French law, it is punishable by up to 5 years imprisonment and fines of up to Euro 300,000.¹⁴⁸ CNIL warned would-be subscribers of 'Did They Read It?' that the use of the service in France could expose them to legal action.

In Germany, the North Rhine Westphalia Data Protection Authority approved a transfer of employee data from Germany to the United States. The authority ruled that General Electric's binding internal

¹⁴⁷ French Data Protection Authorities rule US email spy software unlawful Posted: 18 august 2004
<http://privacydataprotection.co.uk/news/#foreign>

¹⁴⁸ à [l'article 25](#) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui interdit la collecte de données nominatives opérée par tout moyen frauduleux, déloyal ou illicite

rules were sufficient to protect employees' rights during the transfer of data collected by the company's German subsidiary to its US headquarters.¹⁴⁹

The German **Federal Data Protection Act** prohibits the transfer of data to a country that does not provide adequate data protection standards. Section 4(c) of the Act provides that a local Data Protection Authority can approve certain transfers of personal data if the recipient guarantees the protection of the employees' rights, for example, through a contract or binding company rules on conduct. Under Section 4(b), factors to be taken in account when considering a transfer include the purpose of the transfer, the duration of intended use of the data, the countries where the data is collected and will be received and the regulations to be complied with by the recipient. In this case, General Electric's internal rules provided adequate protection, as they specified the purpose for which data would be transferred and granted precise rights to employees including rights to notification and the correction of data.

United States

The **Fourth Amendment**¹⁵⁰ of the US Constitution effectively protects the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures [...]. The **Electronic Communications Privacy Act 1986**¹⁵¹ (ECPA) (Annex 31) sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications. In effect, it prohibits unlawful access and certain disclosures of communication contents. Additionally, the law prevents government entities from requiring disclosure of electronic communications from a provider without proper procedure. Section 2701 of the US Code in which the ECPA is incorporated lays down criminal penalties for those who intentionally access without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.

The case of *Steve Jackson Games, Inc. v. United States Secret Service*¹⁵² involved a seizure of electronic communications and the subsequent review, reading and deletion of files in electronic storage. The Secret Service sought to retrieve a sensitive computer document stolen by computer

¹⁴⁹ German Data Protection Authority allows foreign transfer of General Electric's employee data Posted: 29th December 2003 <http://privacydataprotection.co.uk/news/#foreign>

¹⁵⁰ The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

¹⁵¹ 18U.S.C. Secs. 2510-2711 (1988)

¹⁵² 816 F. Supp. 432 (W.D.Tex. 1993), aff'd, 36 F.3d 457(5th Cir. 1994)

hackers as well as obtain evidence of related criminal activity. The officers had reason to believe that the suspect was an employee of Steve Jackson Games and may have uploaded such documents to the company's computer bulletin board which the suspect used and helped operate. No illegal activity by the company itself was alleged. The officers obtained a warrant to seize a variety of computer files and documents from the company's bulletin board. The trial court found that, despite their denials, the Secret Service officers did in fact read all electronic communications seized including private e-mails not mentioned in the search warrant or affidavit and also deleted some of the seized files. The court held that the officer's conduct with respect to private e-mail failed to comply with the requirements of Title II of the ECPA¹⁵³ relating to the disclosure of the contents of stored electronic communications. The court also declined to find the defendants entitled to a good faith defence for their reliance on the search warrant.

The ECPA contains the general good faith defence of section 2707(e) for reliance on a warrant. In *Davis v Gracey*¹⁵⁴, police officers relied on a warrant to seize the computer equipment from a company whose director was suspected of distributing pornographic material on CDs. The company also ran a bulletin board. The seizure of the stored electronic communications found on the computer equipment at the company, which included communications from bulletin board members, was incidental to the execution of the warrant. To be in good faith, the officers' reliance must have been objectively reasonable.¹⁵⁵ In the discussion of the plaintiff's Fourth Amendment claim, the Court found that the warrant was valid and encompassed the computer equipment. The officers' reliance on the warrant was therefore objectively reasonable and did not breach any ECPA statute.

In *McVeigh v. Cohen*¹⁵⁶ a violation of the "Don't Ask, Don't Tell, Don't Pursue" policy under the National Defense Authorization Act of 1994 regarding military service by homosexuals was alleged and the United States Navy was said to have improperly conducted an investigation of Senior Chief McVeigh based solely on an anonymous electronic mail message the Navy believed to have been sent by Senior Chief McVeigh to a civilian. The court found a violation of the ECPA.¹⁵⁷ Senior Chief McVeigh had not given consent to AOL to give out personal information regarding him to the Navy nor did it obtain a warrant or a court order for the disclosure of such information. The Navy thus

¹⁵³ 18 U.S.C. 2703

¹⁵⁴ 111 F.3d 1472 (10th Cir. 1997)

¹⁵⁵ *Malley v. Briggs*, 475 U.S. at 344-45.

¹⁵⁶ No. 98-116 (D.D.C. Jan. 26, 1998)

¹⁵⁷ AOL is a "provider of electronic communication service or remote computing service" as those terms are used in 18 U.S.C. § 2703(c)(1)(B). The information that Defendants solicited and obtained from AOL concerning Senior Chief McVeigh constitutes "a record or other information pertaining to a subscriber to or customer of" AOL as those terms are used in 18 U.S.C. § 2703(c)(1)(B). Senior Chief McVeigh was a "subscriber to or customer" of AOL at the time Defendants solicited and obtained information about him from AOL.

violated sections 2703(c)(1)(B) and 2707 with full knowledge of the wrongdoing they were committing or with reckless indifference to its lawfulness or unlawfulness. The defendants did not act in good-faith reliance on any of the factors specified in section 2707(e).¹⁵⁸

*Romania*¹⁵⁹

The Romanian Constitution¹⁶⁰ adopted in 1991 recognizes under Title II (Fundamental Rights, Freedoms and Duties) the rights of privacy, inviolability of domicile, freedom of conscience and expression.

Article 26 states, *"(1) Public authorities shall respect and protect intimacy, family and private life. (2) Any natural person has the right to freely dispose of himself unless by this he causes an infringement upon the rights and freedoms of others, on public order or morals."*

Article 27 of the Constitution states, *"(1) The domicile and the residence are inviolable. No one may enter or remain in the domicile or residence of a person without consent. (2) Derogation from provisions under paragraph (1) is permissible by law, in the following circumstances: for carrying into execution a warrant for arrest or a court sentence; to remove any danger against the life, physical integrity or assets of a person; to defend national security or public order; to prevent the spread of an epidemic. (3) Searches may be ordered only by a magistrate and carried out exclusively under observance of the legal procedure. (4) Searches at night time shall be prohibited, except in cases of flagrante delicto."*

Article 28 states, *"Secrecy of the letters, telegrams and other postal communications, of telephone conversations and of any other legal means of communication is inviolable."*

According to Article 30, *"(6) Freedom of expression shall not be prejudicial to the dignity, honour, privacy of person, and the right to one's own image."*

In November 2001, the Parliament enacted Law No. 676/2001 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector¹⁶¹ and **Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of**

¹⁵⁸ Furthermore, the investigation violated Department of Defense regulations because the investigation was not based upon credible information that Senior Chief McVeigh engaged in homosexual conduct, it was not investigated by the officer charged with the duty of conducting the investigation, and the Navy could not identify any alleged statement within the meaning of the regulations made by Senior Chief McVeigh that he was a homosexual.

¹⁵⁹ Entire Chapter on Romania courtesy of Bogdan Manolea, www.legi-internet.ro

¹⁶⁰ <http://www.cdep.ro/pls/dic/act_show?ida=1&idl=2&tit=2#t2c2s0a26>.

¹⁶¹ <<http://www.riti-internews.ro/lg676.htm>>.

Such Data.¹⁶² These laws follow very closely the European Union Telecommunications Privacy (1997/66/EC) and Data Protection (1995/46/EC) Directives respectively.

Law No. 676/2001 provides for specific conditions under which privacy is protected with respect to the processing of personal data in the telecommunications sector. The law applies to the operators of public telecommunications networks and the providers of publicly available telecommunications services who, in the context of their activities, carry out processing of personal data. The regulatory authority established by Law No. 676/2001 was originally the Ministry of Communication and Information Technology, but it was changed by the Government Emergency Ordinance No. 79/2002 for the National Regulatory Authority for Communication (NRAC).¹⁶³ No specific department was created to take care of the application of Law 676/2001.

In 2004 Law 676/2001 is practically replaced by **Law 506/2004** (Annex 32) closely following Directive 2002/58/CE of the European Parliament and the Council on personal data processing and privacy protection in the electronic communication sector, published in the Official Journal of the European Community no.L.201/31.07.2002.

The new law entered in force on 17 November 2004 and it divides the task of enforcing the law, between two institutions: the National Regulatory Authority for Communication (NRAC) for issues related to electronic communications and the People's Advocate Office for issues related to privacy. In this sense, the National Regulatory Authority for Communication (NRAC) has attributions related to security measures for electronic communication, non-compliance with invoice issuing conditions, infringement of the obligations regarding the presentation and restriction of calling and connected line identification.

On the other hand, the People's Advocate Office has attributions related to listening, recording, storing and any other form of interception and surveillance of communications and related traffic data, use of an electronic communication network with the purpose of storing the thus stored information in the terminal equipment of a subscriber or user or obtaining access to it, traffic data processing, location data processing, subscriber directories and sending Spam.

Law No. 677/2001 applies to the processing of personal data done, totally or partially, through automatic means, as well as to the processing through means other than automatic, which are part of, or destined for, an evidence system.

¹⁶² <<http://www.avp.ro/leg677en.html>>.

¹⁶³ <<http://www.anrc.ro/en/index.htm>>.

The supervisory authority for Law No. 677/2001 is the Ombudsman (also called "The People's Advocate").¹⁶⁴ The Organizational and Functional Regulations of the Ombudsman were changed in order to provide for the creation of a special Private Information Protection Office (PIPO), concerned with the protection of individuals in relation to private data processing. This specialized structure established for the implementation of the data protection legislation should have 19 posts.

The implementation of the legislation in the personal data protection domain was subject to criticism in the last report of the European Union: "2004- Regular Report On Romania's progress towards accession "¹⁶⁵ which stated that "*progress in implementing personal data protection rules has only been limited. There are grounds for concern regarding the enforcement of these rules: enforcement activities are far below levels in current Member States and additional posts have not been filled during the reporting period*" and that "*as regards enforcement and administrative capacity, contrary to the announcement of June 2003 that the number of positions in the Directorate for the Protection of Individuals' Rights as regards Personal Data Processing (part of the office of the Romanian People's Advocate) would be increased to 20, the actual staffing level remained at 14 employees.*"

According to the People's Advocate web site in April 2005, presently there are 15 people working in this division. The situation significantly improved in 2004, when the number of people employed within the personal data protection division of the People's Advocate institution increased. Also, the activity of promoting personal data protection and the obligations related to this domain, on the occasion of several seminars meant for specific sectors (hotels, tourism, Internet services, health, financial-bank etc), has also increased significantly (5 times as compared to 2003) the number of registered personal data processing operators.¹⁶⁶

The Ombudsman adopted several orders in 2002 in order to apply Law No. 677/2001.¹⁶⁷ In 2003 the Ombudsman proposed a normative act establishing a notification fee. To that effect, Law No. 476/2003 was adopted.¹⁶⁸

¹⁶⁴ <<http://www.avp.ro>>.

¹⁶⁵ Available at http://europa.eu.int/comm/enlargement/report_2004/pdf/rr_ro_2004_en.pdf

¹⁶⁶ Bogdan Manolea - **Institutional Framework for Personal Data Protection in Romania**, presented at [Conference "Personal data Protection – Policy and Practice Practice in the EU Accession and New Member States", 8 April - Sofia](#). Document available at http://www.apti.ro/DataProtection_ro.pdf

¹⁶⁷ Ombudsman Order No. 52 (April 18, 2002) for the approval of the minimum security measures for data processing laying at the basis of the operators adopting technical and organizational measures to guarantee a proper legal security level of data processing, Official Monitor, June 5, 2002; Ombudsman Order No. 53 (April 18, 2002) for the approval of standardized notification forms, Official Monitor, June 5, 2002; Ombudsman Order No. 54 (April 18, 2002) for the determination of situations requiring the notification of data processing that falls under Law No. 677/2001, Official Monitor, June 5, 2002; Ombudsman Order No. 75 (June 4, 2002) to establish specific measures and procedures to provide a satisfactory level of protection for data subjects, Official Monitor, June 26, 2002.

¹⁶⁸ Official Monitor, No. 814 of November 18, 2003.

The complaints are solved according to Article 25 Law No. 677/2001. Pursuant to these provisions, the complaint cannot be submitted to the supervisory authority earlier than 15 days from the time a complaint is submitted, that deals with the same problem, to the data controller. In order to solve the complaint, the supervisory authority may listen to both the respective person and the data controller or, if applicable, the person who represents the interests of the respective persons. If the complaint is justified, the supervisory authority is empowered to order the temporary interruption or ceasing of the data processing, the partial or total erasure of the processed data, and may also notify the criminal bodies or bring a lawsuit.¹⁶⁹

As a rule a complaint cannot be addressed by the supervisory authority if a judicial procedure with the same parties and same subject matter has been already initiated and if the petitioner does not provide a proof of previously approaching the data controller.

In case the supervisory authority notices the inconsistency with the provisions of the Law no. 677/2001, it may partially or totally delete, suspend or terminate the data being processed and may notify the criminal prosecution bodies or may file complaints to a court of law. Also, for some acts of infringement of the law, it may be disposed contravention sanctions liable to a fine.¹⁷⁰

In 2003, the Ombudsman issued Order No. 6 of January 29, 2003 that establishes standard contractual clauses for the transfer of personal data to third countries that do not provide an adequate level of protection.¹⁷¹

For the period July 1, 2004 – April 22, 2005, there were registered 1303 notifications filled by 1204 data controllers. For the notifications regarding the international transfers of personal data 49 authorisations were issued. For the same period 4 investigations were conducted, to data controllers from public and private sector. In the case of the 17 complaints filled according to the Law no. 677/2001 on the protection of persons concerning the processing of personal data and free circulation of such data, were claimed possible infringements of the rights guaranteed by this law, in the field of activities for the processing of personal data in the field of finance – banking or direct marketing.¹⁷²

The total number of data controllers registered till now with the supervisory authority is 2381.¹⁷³

¹⁶⁹ E-mail from Ioan Muraru, People's Advocate to Cédric Laurant, Policy Counsel, Electronic Privacy Information Center (EPIC) (July 4, 2004) (on file with EPIC).

¹⁷⁰ E-mail from **Virgil Cristian Cristea**, Director to Ula Galster, Policy Counsel, Electronic Privacy Information Center (EPIC) (April 27, 2005) (on file with EPIC).

¹⁷¹ Official Monitor No. 151, March 10, 2003.

¹⁷² E-mail from **Virgil Cristian Cristea**, *supra*.

¹⁷³ E-mail from **Virgil Cristian Cristea**, *supra*.

In the Activity Report of the People's Advocate Institution for 2004, Chapter 4 is dedicated to the *Activity of the People's Advocate as a supervisory authority for personal data processing*. The report was submitted for debates to both Chambers of Parliament on January 31, 2005.

The report for 2004 of the People's Advocate Office¹⁷⁴ states that *“as compared to 2003 there is a visible progress; the number of personal data processors increased 5 times and the number of notifications increased by 300%. Until now, a total of 97 notifications have been registered having as object personal data transfer abroad. Out of these, in 2004, 57 transfer notifications were registered. The progress is remarkable in this sector also as compared to the previous years, the notifications for transfer abroad of personal data having increased by 196.5%, as compared to 2003. For the transfer abroad of personal data, in 2004, 53 authorizations were issued out of the total of 66.”*

According to the 2004 Report, the People's Advocate provided 943 consultations by phone or in writing for the enforcement of the obligations foreseen by the law 677/2004. Also the People's Advocate has approved 2 codes of conduct that included specific norms for the protection of personal data. The 2 codes of conduct were adopted by the Association of Leasing Companies from Romania¹⁷⁵ and by Direct Marketing Romanian Association.¹⁷⁶

In 2003 the Ombudsman only ordered four prior controls and eight investigations, performed both at public and private operators.¹⁷⁷ In 2004, three investigations and three preliminary controls were carried out. In 2004, the supervisory authority received four claims, most of them involving the sending of unsolicited commercial messages (spam) by direct marketers.¹⁷⁸

All these lacks in the enforcement of the law on data protection did not imminently concern the Romanian Government. However, the occurrence of these lacks in the European Union country report for 2004 made the authorities in Bucharest anxious.

Thus, in a short time, within the Consultative Council of 30 August 2004 for integration into EU – the Ministry of Internal Affairs, the Ministry of EU Integration and the People's Advocate discussed the data protection issue. Even though no representative of the NGO sector was invited, one of the

¹⁷⁴ Romanian Ombudsman Annual Report 2004 available at < <http://www.avp.ro/statnoie.html>>

¹⁷⁵ Notice n. 2 / 15 June 2004 published in the Official Monitor no. 627 from 9 July 2004

¹⁷⁶ Notice n. 3 / 15 September 2004 published in the Official Monitor no. 874 from 24 September 2004

¹⁷⁷ In a public statement the President of the Ombudsman, Ioan Muraru, declared that the designation of this institution as the surveillance authority for personal data processing is against the purpose of this institutions and asked the Parliament to transfer these tasks to other public institutions. He believes that such an institution requires very specialized personnel and the Ombudsman does not and cannot have such structures. He asked for a specialized Control Authority on Personal Data Processing. "Avocatul Poporului își declină competențele privind protecția datelor cu caracter personal" (The Ombudsman Declines Responsibilities on Personal Data Protection) Azi, February 13, 2004, available at <<http://www.azi.ro/archive/2004/02/13/social.htm#stirea2>>.

¹⁷⁸ E-mail from Ioan Muraru, *supra*.

conclusions of the meeting was that *“civil society can play a bigger role in informing the people on personal data protection and to support the public administration in this field”*.¹⁷⁹

A draft act on the creation, organization and operation of the National Authority for the Surveillance of Personal Data Processing was quickly prepared and available for public comments on the Ministry of EU Integration website on 9 October 2004.¹⁸⁰ The same draft unmodified was submitted to the Parliament for discussions on 7 December 2004.

The act aims to establish the “National Authority for the Control and Supervision of Personal Character Data Processing” (ANSPDCP). The New Authority shall have at its disposal all necessary resources (logistical, human capital-dedicated specialists, administrative structures, as well as financial means) in order to ensure an efficient and correct promotion and implementation of the Law. The Authority shall have a President with the rank of Ministry and a Vice-President with the rank of Secretary of State, both appointed by the Romanian Senate (the Romanian upper Parliamentary Chamber). The Permanent Bureau of the Senate shall appoint the candidates for the 2 positions, after consulting the proposals addressed by the parliamentary groups from the 2 Parliamentary Chambers. In order to ensure continuity in the activity of data protection, the draft law stipulates that the New Authority shall become operational in 90 days after the Law comes into force and stipulates clear responsibilities for the new institution. It also regulates the transfer of the database from the People’s Advocate Office to the New Authority.¹⁸¹

The proposed draft is, without any doubt, one step ahead to a better protection of personal data if it is only for the creation of an independent state institution, with a president and vice-president appointed by the Senate, for a 5-year period. The possibility of employing a number of maximum 50 people within this authority is also foreseen.

Some critics of the draft law that wants to establish the “National Authority for the Control and Supervision of Personal Character Data Processing” (ANSPDCP) were made with several occasions.

¹⁸²

The Chamber of Deputies approved on 8 March 2005 the proposed draft on establishing the “National Authority for the Control and Supervision of Personal Character Data Processing” (ANSPDCP), in its

¹⁷⁹ See the press release at http://groups.yahoo.com/group/romania_eu_list/message/16950

¹⁸⁰ Ministry of European Integration – www.mie.ro

¹⁸¹ Precu, Corneliu, "Romanian Data Protection Legislation in a European Context", 2005, Master Thesis, The Master Programme in Law and IT, Stockholm University.

¹⁸² See for example and details Bogdan Manolea - **Institutional Framework for Personal Data Protection in Romania**, presented at [Conference “Personal data Protection – Policy and Practice Practice in the EU Accession and New Member States”, 8 April - Sofia.](#) Document available at http://www.apti.ro/DataProtection_ro.pdf

initial form. Although a series of amendments or re-discussions have been proposed by the opposition members, they were rejected due to procedural matters or for non compliance with EU requirements.

In addition, the declaration of the People's Advocate at the plenum of the Deputy Chamber¹⁸³ meant to support this normative act makes doubtful the intention of the government and of the People's Advocate of treating this matter seriously:

*" I want to inform you that the experts in Brussels have agreed with the draft, to the letter, there are reports from Brussels, therefore, these drafts were accepted only after the conviction was created in Brussels that this authority will be entirely autonomous, totally independent. And this autonomy and independence, eventually, was approved, to say so, only if the president and vice-president will be appointed by a parliament assembly so that it may be no subordination to the Government or the ministries (...). No doubt you can bring, I know, improvements, amendments. I repeat, within the report that has been sent from Brussels, which exists with the documents submitted by the Government to the Parliament, it is very clear, sometimes, I repeat, to the letter, how such a project should look like. It is a question that is related to our acceptance in the European Union if I may say so although this matter is beyond me somehow."*¹⁸⁴

The Draft act was adopted by the Senate with no changes on 11 April 2005. Finally the law was signed by the Romanian President on 3 May 2005 and has become Law no 102/2005.¹⁸⁵

In 2001, Law No. 682/2001 was enacted to ratify the Council of Europe (CoE)'s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108). By Law no. 55/2005 was ratified the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, adopted in Strasbourg on November 18, 2001.¹⁸⁶

In 2002, Law No. 365/2002 on Electronic Commerce¹⁸⁷ adopted the opt-in principle for unsolicited commercial e-mails ("spam").¹⁸⁸ In 2002, the National Audiovisual Council¹⁸⁹ issued regulations regarding privacy and television and radio programs in Decision No. 80 of August 13, 2002 Regarding the Protection of Human Dignity and the Right to Protect One's Own Image established a few privacy

¹⁸³ Available at <http://www.cdep.ro/pls/steno/steno.stenograma?ids=5812&idm=6> (Only in Romanian)

¹⁸⁴ The declaration of the People's Advocate at the plenum of the Deputy Chamber

¹⁸⁵ Official Monitor, No. 391 of May 9, 2005. Text available at < http://www.legi-internet.ro/autoritate_date_pers.htm> (only in Romanian)

¹⁸⁶ E-mail from **Virgil Cristian Cristea**, *supra*.

¹⁸⁷ Available at <<http://www.legi-internet.ro/en/e-commerce.htm>>.

¹⁸⁸ Art. 6 (1) provide that "commercial communications through electronic mail are forbidden, except where the recipient has expressly consented to receive such communications."

¹⁸⁹ Homepage <<http://www.cna.ro>>.

principles: Article 6 states, "(1) *Any person has a right to privacy, privacy of his family, his residence and correspondence. (2) The broadcasting of news, debates, inquiries or audio-visual reports on a person's private and family life is prohibited without that person's approval.*" According to Article 7, "*It is forbidden to broadcast images of a person in his or her own home or any other private places without that person's approval; (2) It is forbidden to broadcast images of a private property, filmed from the inside, without its owner's approval.*"

The interception of telephone calls, the opening of correspondence and other similar actions are regulated by Law No. 51/1991 on National Security in Romania and Law No. 26/1994 on Police Organization.¹⁹⁰ Article 13 of Law No. 51/1991 allows the interception of calls in case of crimes against the state, only as a result of a mandate issued by the General Prosecutor of the Office related to the Supreme Court. The mandate has a duration of six months maximum with the possibility of being extended by up to three months by the General Prosecutor. According to Article 16 of the same law, the means to obtain information may not infringe citizens' fundamental rights and freedoms, *i.e.*, their private life, honor or reputation, or to subject those rights and freedoms to legal restrictions. The citizens who consider that their rights have been infringed, can appeal to the Commissions of Human Rights of the 2 Chambers of the Parliament. According to Article 17 of Law No. 26/1994 that aims at preventing organized crime and serious infringements in the interest of a criminal investigation, the police can require the Prosecutor's Office to intercept calls and open correspondence pursuant to Law No. 51/1991.

In 1996 the Criminal Code was modified by Law No. 41/1996 that introduced a new section on the use of audio and video recordings for interception purposes. The section establishes the conditions under which video and audio recordings may be carried out, including the interception of telephone calls. Therefore, according to Article 91 of the Criminal Code, the recordings on magnetic tape can be used as evidence if the following conditions are complied with: there are reasons to believe that a crime has been, or is about to be, committed; the criminal deed related to which the recording is made is a crime investigated *ex-officio*; the use and efficiency in finding out the truth; the authority that carries out the wiretap has been properly authorized to do so. The authority competent to issue such an authorization is the prosecutor designated by the General Prosecutor of the Office related to the Court of Appeals. The authorization to wiretap is given for a period of up to 30 days.

The law also compels law enforcement authorities to report specific information about their wiretapping: the authorization given by the prosecutor, the number of the telephones between which

¹⁹⁰ Nicolae Volonciu, *Penal Procedure Treatise*, 509-514 (Ed. Padeia 1999).

the calls take place, the names of the people carrying out the conversations, and, if known, the date and time at which each communication took place, and the item number of the roll or tape on which the recording is made.

Similar provisions related to the recording of traffic data were introduced by the Law on Anti-Corruption No. 161/2003¹⁹¹ in order to prevent and combat cyber-crime. Romanian law does not provide for the retention of traffic data by Internet service providers (ISPs). The law provides that, only in emergency and properly motivated cases, law enforcement can expeditiously obtain the preservation of computer or traffic data if they could be destroyed or altered, and if there are good reasons to believe that a criminal offence by means of computer systems is being, or is about to be, committed, and for the purpose of gathering evidence or identifying the wrongdoers. During the criminal investigation, the preservation is undertaken by the prosecutor, pursuant to an appropriate ordinance and at the request of the investigative body or ex-officio, and during trial, by a court settlement. This ordinance is valid only for no longer than 90 days, and can be exceeded only once by a period not longer than 30 days.

Most of the cases involving invasion of privacy concerned the illegal interception of telephone calls. Several complaints were filed, especially by Opposition's members.¹⁹² The president of the Senate Human Rights Commission recently declared¹⁹³ that a hearing of those people who complained on these issues should take place in the Commission. The Foundation Horia Rusu organized a public debate on those issues on 14 April 2003.¹⁹⁴ Two Opposition deputies presented a draft law¹⁹⁵ that would establish the conditions pursuant to which telephone calls could be intercepted so as to limit the intrusion into people's privacy. The draft provides that the warrant authorizing interception could be issued only by a judge and that, later on, the person wiretapped would have to be informed about the reasons of wiretapping. Other cases involved the invasion of privacy of several Romanian TV stars.¹⁹⁶

In the beginning of 2005 several cases were shown in the press that the Romanian secret service intercepted phone calls of journalists and other public persons.

On 27 January 2005 the Chief of the Romanian Secret Service (SRI) Ioan Timofte explained¹⁹⁷ that several phones of some Romanian and foreign journalists in Romania were intercepted for several

¹⁹¹ Official Monitor No. 279, April 21, 2003, available at <<http://www.legi-internet.ro/en/cybercrime.htm>>.

¹⁹² Such as Dan Carlan, vice-president of the Liberal Party; Iasi Count, Dorin Marian, ex-counsellor of the former President Emil Constantinescu.

¹⁹³ Roxana Ristache, "Interception of Telephone Calls from Iasi in Attention of the Senate," Cotidianul, April 16, 2003.

¹⁹⁴ Ovidiu Banches, "The Citizen Threatened by National Safety," Ziua, April 15, 2003.

¹⁹⁵ Draft law No. 207/2002 amending Law No. 51/1991 on the National Security of Romania.

¹⁹⁶ "Extensions of Free Speech against Privacy?" Cotidianul, April 19, 2002, available at <<http://www.cotidianul.ro/anterioare/2002/reportaj/rep1521apr.htm>>.

¹⁹⁷ Dan BUCURA, Gabriela STEFAN, "There are paid and recruited journalists by foreign information services. ", Adevarul, 27 January 2005

months as they were being suspected of sabotage and crimes against Romanian National security. The Romanian Press Club and the Board of the Foreign Press in Romania Association have protested¹⁹⁸ and demanded SRI to publicly announce the name of the journalists that were supervised. SRI refused, considering that they cannot reveal secrets that may affect national security. The Defense Commissions in the Romanian Parliament, after a hearing of the people involved have considered that the interceptions were legal.¹⁹⁹

Claiming that an investigation was undergoing for Judge Andreea Ciuca, ex-president for the Mures Tribunal, the Anticorruption Prosecutor (PNA) from the Mures County monitored the phones of over 70 local journalists, local and national press headquarters and lawyers for over 13 months during 24.04.2003 - 25.05.2004.²⁰⁰ No relevant information was offered by PNA to explain this case.

Even the UK liberal MEP Emma Nicholson has accused the Romanian secret service of spying on her. Emma Nicholson said that the surveillance was "predictable and obvious", according to an article in Austria's Der Standard on 8 February 2005. Her comments follow similar ones made by former Dutch MEP Orië Oostlander last week. Mr. Oostlander, a Christian Democrat and also involved in drawing up reports on Romania, alleged that he had been under surveillance by the Romanian secret service.²⁰¹

AVAILABILITY

Availability ensures no denial of authorised access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category. Availability relies heavily on access to the network and thus that interconnection is guaranteed. Interconnection covers the physical and logical linking of networks and is an essential element in any multi-network environment. It enables the users on one network to communicate with users on other networks or to access services provided by other networks. For developing countries, it is essential as interconnection to the incumbent operators network is critical for successful market opening in newly liberalized markets.²⁰²

European Union

¹⁹⁸ Hotnews.ro " SRI does not publicized the names of the surveilled journalists " from 1st February 2005 available at http://www.hotnews.ro/articol_14162-SRI-nu-face-publice-numele-ziaristilor-urmariti.htm

¹⁹⁹ Ion M. IONITA, "Virgil Ardelean pretends that the intention to intercept journalists calls started from a provocation", Adevarul, 27 January 2005.

²⁰⁰ Adina Anghelescu, Razvan Savaliuc, "PNA has illegally intercepted the journalists phones " Ziua 03 feb 2005

²⁰¹ Honor Mahony, "Romanian secret service accused of spying on MEP", euobserver.com 8 February 2005

²⁰² Policies: e-Communications, Interconnection and Interoperability, Europe's Information Society Thematic Portal, European Commission, http://europa.eu.int/information_society/policy/ecomm/todays_framework/interconnection_interoperability/index_en.htm

All operators of public communications networks in the EU have both a right and a duty to negotiate interconnection with each other. In the event of a dispute, the national regulatory authority (NRA) may intervene. Under the 1998 regulatory framework, incumbent operators were required to provide interconnection according to the principles of transparency, non-discrimination and cost orientation and to publish a Reference Interconnection Offer containing the relevant terms and conditions. The Commission recommended the use of forward-looking long run incremental costs (FL-LRIC) as the most appropriate costing methodology for fixed network interconnection and published a series of 'best current practice' prices for NRAs to use as guidelines when assessing interconnection charges.

These former obligations are carried forward to the current regulatory framework until an NRA undertakes a market analysis and maintains, amends or withdraws the former obligations. NRAs have more flexibility under the current framework in terms of the precise remedies imposed on operators with significant market power in particular markets.

The Commission Recommendation on relevant markets identifies call origination, call termination and transit as markets that need to be analysed separately by NRAs.

Directive 2002/19 (Annex 33) the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities is the Access Directive.²⁰³ The Access Directive lays down a procedural framework for national regulation authorities to follow and identifies factors to be taken into account when granting access but does not specify precise access obligations. In general access obligations are only imposed on operators that have significant market power in specific markets as a means of remedying a particular market failure, but there is also provision for access to be imposed by authorities in pursuit of broader public policy objectives.²⁰⁴

A **Council Framework Decision on Attacks Against Information Systems** designed to protect critical information infrastructure security²⁰⁵ was introduced in May 2002. This EU decision is mainly understood as a defence as well as a EU/national security issue. It proposes the following as descriptions of threats against information systems, a terminology defined in the broadest sense possible, to include recognition of the convergence between electronic communication networks and the various systems to which they are connected: unauthorised access and disruption of information systems (this would explicitly include DoS attacks), execution of malicious software that modifies or

²⁰³ see Directive 2002/20 of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services, also known as the Authorisation Directive

²⁰⁴ Supra 15

²⁰⁵ Supra 15

destroys data, interception of communication and malicious representation. In response to 9/11, two more specific offences have been added, namely serious attacks through illegal access to information systems and serious attacks through interference with information systems.²⁰⁶ This Framework certainly goes a long way from the CMA in being more extensive and inclusive and appears very different to UK legislation adopted in past years. However, the very real threat of attack has pushed the EU to seriously consider the implications of a future attack on European systems.

All the criminal offences covered in the framework decision require the element of intent. The term intentional is used explicitly in Articles 2, 3 and 4. Consequently, the Framework Decision does not criminalize actions where there is gross negligence or other recklessness.

Without right is defined as access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the national legislation.²⁰⁷ Article 3 covers illegal interference with information systems²⁰⁸ and Article 4, illegal data interference. Article 5 puts an obligation on Member States to ensure that even activities secondary to offences against information systems are punishable. Article 5 places heavy emphasis on the intent. Criminalizing attempt effectively shifts the weight of the crime from commission of the offence to the *mens rea* in a preventative effort.

Council of Europe

The Council of Europe **Convention on Cybercrime** 2001 also covers data and system interference. Article 4 covers the damaging, deletion, alteration and suppression of computer data. The interest in protecting such data is to preserve integrity and availability through the proper functioning and use of computer data. Alteration effectively requires a modification of the quality of the information. Alteration also includes the addition of data without previous erasure. The term suppression effectively terminates the availability of data and is thus included in this definition. This consequently includes

²⁰⁶ Ibid

²⁰⁷ Article 1

²⁰⁸ (a) *the serious hindering or interruption, without right, of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data computer data. The elements of inputting or transmitting computer data specifically address the problem of so-called "denial of service attacks" where there is a deliberate attempt to overwhelm an information system. The offence also covers the "interruption" of the functioning of an information system, which could be inferred from the phrase "hindering" but is included here explicitly for the sake of clarity. The other elements in the offence (damaging, deleting, deteriorating, altering or suppressing computer data) specifically address the problem of viruses, and other types of attacks, which are directed at hindering or interrupting the functions of the information system itself.*

(b) *the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person. This covers virus attacks aimed at the content (or computer data) on the information system, as well as corruption of web-sites.*

any running of malicious software such as viruses, worms and logic-bombs capable of altering or damaging data.

Article 5 covers the serious hindering of the functioning of a computer system, by inputting, transmitting, damaging, deleting, deteriorating, altering and suppressing computer data. Interference influences the activity performed by a computer system or renders it inoperative. This can have an effect on the processing capability of the system. Interfering, for example, with government and other public bodies can have disastrous effects. Interference with critical infrastructures can represent a significant threat to the politico-economic well being of a country and its society. Thus hindering and interrupting with computer systems constitutes a criminal offence.

Of all attacks directed against ISPs, 80% are DoS attacks whereas only 20% are hacking or penetration attacks.²⁰⁹ The particularity of DoS attacks is that they flood a certain IP address, such as a website, with huge amounts of traffic causing the site to overload and crash. As a result, legitimate users who want to access the site are not able to do so and are thus denied service. These types of attacks are sometimes distinguished with difficulty from a genuine high peak in traffic. DoS attacks were brought to world-wide attention in February 2000 when several huge attacks were directed at some of the world's premier e-commerce websites, namely Yahoo!, Ebay and Amazon, causing significant financial losses²¹⁰. Numerous sites were rumoured to have been affected. This type of attack, when in huge numbers, is called Distributed DoS attacks (DDoS). In these types of attacks, the perpetrator has at his command several hundreds or even thousands of computers which he has infected with a "bot" which is an application that performs some action on behalf of a remote controller²¹¹, i.e. the perpetrator. Often this type of software reproduces itself and sniffs around looking for more vulnerable hosts to infect²¹². The software is accordingly able to propagate itself rapidly and enables the perpetrator to have at his disposition hundreds to tens of thousands of infected hosts forming a cluster, or network, of bots subsequently named botnets. The software then waits for the command from the central client (the perpetrator) to 'attack' a named site with an overwhelming amount of 'hits' or request for information from that site.²¹³

²⁰⁹ Ibid

²¹⁰ Denial-of-Service Attacks Rip the Internet by Lee Garber in Technology News, Computer Magazine

²¹¹ Internet Architecture WG: DoS-resistant Internet Subgroup Report by Mark Handley, University College London

²¹² Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks by Cisco Systems

²¹³ Denial of Service prosecution in the UK, January 19, 2005 at Out-Law.com

United Kingdom

In the UK, under the **Computer Misuse Act 1990**, there was a first court prosecution against teenager Aaron Caffrey who faced charges under the CMA for a DoS attack. However, the merits of the Act as pertaining to DoS attacks were not argued because the defence convinced the jury that Caffrey had not launched the attacks but had been a victim of a zombie computer as hackers had managed to install a Trojan on his system and effectively launch attacks from his computer. Caffrey was duly acquitted.²¹⁴

There has, however, been a more recent arrest outcome of which will be interesting in setting a hopefully justifiable precedent for DoS offences. The arrest concerns a Scottish man who appeared in Elgin Sheriff Court on January 18th 2005 facing charges under the CMA for launching DoS attacks. After a collaboration called Operation Casper between the NHTCU and US Secret Service, they managed to track down the culprit who had been carrying out attacks against companies in Scotland and the US as part of an extortion plot. The results of the trial will not be known before the end of the year and thus it remains to be seen whether the courts will be successful in applying the CMA to DoS attacks and making it an offence.

On the other hand, the Convention on Cybercrime as presented by the Council of Europe includes non-EU countries such as the US and Japan, as well as other nations, making it a 43-nation international treaty.²¹⁵ The Convention establishes common definitions and criminal penalties for offences such as unauthorised computer intrusion, DoS attacks and the dissemination of computer viruses and worms.

Article 6 of the Convention criminalizes the misuse of devices for the purpose of committing illegal access or interception, or data and system interference. This includes the possession, production, sale, and procurement for use, import, distribution or otherwise making available of such items for the purpose of committing such crimes. Tools such as viruses and other malicious software pose a dangerous economic threat to all societies dependant upon the Internet.

Another privacy problem of which countries should be aware of is spyware and adware. Spyware can be defined as a piece of software that employs a user's Internet connection in the background without their knowledge and gathers and transmits information on the user or their behavior.²¹⁶ Adware is any

²¹⁴ Supra 27

²¹⁵ Supra 23

²¹⁶ [PestPatrol] [Current Developments in Adware and Spyware](http://eric_goldman.tripod.com) Eric Goldman Marquette University Law School eric_goldman@marquette.edu http://eric_goldman.tripod.com

software application in which advertising banners are displayed while the program is running and which brings targeted ads to your computer after providing initial consent.²¹⁷

United States

Under US law, such software intrusion is dealt with by the **Computer Fraud & Abuse Act** (Annex 34),²¹⁸ the **Electronic Communications Privacy Act**, contract law and trademark law. One good example is the **Utah Spyware Control Act**²¹⁹ (Annex 35) which restricts the installation of spyware and the use of context-based triggering mechanisms to display pop up advertising. Such a mechanism infers the context from keywords typed into the navigation bar or in search engines. The law excludes, however, software which specifically asks for user consent. A proposed federal law, the Securely Protect Yourself Against Cyber Trespass (SPYACT) Act,²²⁰ would effectively restrict such software from taking control of a computer, modifying Internet settings, keystroke logging, bad installation procedures, obtaining personally identifiable information (PII) through misrepresentation and disabling protective software. It would also define user consent standards for “information collection programs”.²²¹ Other proposed federal laws include the SPYBLOCK Act²²² which would restrict downloading software onto a computer unless it meets standards for disclosure. Also, specific requirements for uninstalling software would be imposed. The Controlling Invasive and Unauthorized Software Act²²³ was introduced in February 2004 but appears to have been rolled into SPYBLOCK Act. Additionally, the proposed Computer Software Privacy and Control Act²²⁴ would restrict collecting and transmitting Personally Identifiable Information, monitoring web activity, changing default settings, using software to display ads and transmitting software based on misleading notices. Similarly to the SPYACT, it would specify standards for obtaining user consent. Also, the proposed Internet Spyware (I-SPY) Prevention Act of 2004²²⁵ criminal penalties for unauthorized loading of software onto a computer and then transmission of personal data for harmful purposes. The I-SPY Act is intended to punish spyware without placing undue burdens on legitimate uses of the same or similar technology. The law would make it a crime to cause computer code or programs to be copied onto a computer to further another federal offense, to perform identity theft; or to impair the security

²¹⁷ Ibid

²¹⁸ 18 U.S.C. section 1030(a)92) : unauthorised access to obtain information

²¹⁹ Utah Code sections 13-39-101 to 401 (March 2004)

²²⁰ “SPY Act” (HR 2929, Bono) initially introduced as Safeguard Against Privacy Invasions Act

²²¹ Ibid

²²² S.2145, Burns/Wyden

²²³ S.2131, Burns

²²⁴ HR 4255, Inslee

²²⁵ HR 4661, Goodlatte

protections of the computer. Penalties for breaking the law would run from two to five years in prison, in addition to fines.

Developing countries should eventually look to spyware and adware control mechanisms, as they are a dangerous invasion into user's privacy. However, as few laws exist to date, it is still too early to judge whether such legislation as proposed in the US will effectively limit the harm that such software has caused to user privacy. However, much criticism coming from the media, professionals and individuals has already been directed at such legislation alleging that attempts to regulate technology will fail, that many software vendors will spend wasted money on compliance and that plaintiffs will celebrate any law creating a private cause of action. Additionally, it has been predicted that consumers will be bombarded with unhelpful poorly drafted disclosures that they mindlessly click through and will continue to lose faith in all click through agreements. Constitutional challenges will plague any law for years, and many laws (especially state laws) will ultimately be found unconstitutional.²²⁶ These are some of the very negative predictions, but which are not wholly unfounded if the CAN-SPAM Act is anything by which to measure it. It would be perhaps safer to prioritize technical measures while observing the effect that anti-spyware legislation will have in the US before implementing similar legislation.

²²⁶ Supra 39

4. CYBERCRIME

COMPUTER RELATED CRIME

Computer-related crime, otherwise known as cybercrime, refers to attacks against the infrastructure of computer systems on the Internet or private networks. Crimes such as online practices of forgery and fraud are also considered as cybercrimes. The digital world has enabled the use of computers and other communication tools not only as weapons from which traditional crimes can be committed, but also the creation of new crimes brought about by the very existence of such technology. And for these new crimes, older legislative instruments have become inadequate and difficult to apply to such an environment. Developing countries have become ideal breeding grounds as well as targets for online criminals. This is mainly due to the fact that many of these countries are new to the online environment and technology in general. This is added to the rapid development and proliferation of advanced technological tools, software and know-how through ICTS. Developed countries themselves have only started dealing with these issues in the past decade or so, and it is a fact that technology progresses at much faster pace than legislative bodies and governmental authorities respond. It is therefore not surprising that many criminals seek haven in countries where cybercrime laws do not yet exist in order to commit criminal acts without fear of criminal sanctions. Consequently, the more immediate concern is to elaborate and implement legislation which will be able to deal with cybercrime appropriately. Several international conventions exist which already try deal with these new, sometimes complex, issues and adopt an appropriate framework for them.

International

The United Nations **Resolutions 55/63²²⁷ and 56/121²²⁸ on Combating the Criminal Misuse of Information Technology** (Annex 36) resolutions tried to address the problem of safe havens for those who criminally misuse information technologies by requesting that States put into place laws to eliminate such havens. Recommendations included increased cooperation in law enforcement during investigation and prosecution of computer-related crime, the protection of confidentiality, availability and integrity of computer systems from unauthorised impairment by the legal system. Preservation of data in investigations of such crimes was an important concern as well fast access to such data and the penalization of criminal abuse.

Two further resolutions were adopted, Resolutions 57/239 and 58/199²²⁹ on the Creation of a Global Culture of Security and the Protection of Criminal Information Infrastructure.

²²⁷ 4 December 2000

²²⁸ 19 December 2001

²²⁹ 23 December 2003

The first resolution focused principally on the need for States to take action domestically on nine goals: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment. The second resolution noted the interdependence on information infrastructures with other sectors of global infrastructure critical for public services. The Annex to the resolution listed different elements for protecting critical infrastructures.

The Eleventh UN Congress on Crime and Prevention and Criminal Justice which took place in April 2005 undertook a Workshop (6) which looked at measures to combat computer-related crime. The Workshop report identified several different types of computer-related crime and has tried to elaborate a conceptual model with regard to definitions of cybercrime. This included illegal criminal conduct in the case of crimes directed at computing and communication technologies themselves, crimes involving the use of digital technologies as well as crimes involving the incidental use of computers with respect to the commission of other crimes, making the computer a source of digital evidence. Crimes that target ICTs include theft of telecommunications and computer services by using hacking techniques in order to gain unauthorized access, password cracking, digital cloning, and credit card fraud. Other conduct, such as denial of service attacks, can effectively crash servers and websites, but this has been dealt with under the availability chapter.

European Union

Steps were also taken at the EU level. Article 29 of the Treaty on the European Union²³⁰ effectively provides for the prevention of crime, organised or otherwise, as a means of achieving the Union's objective of offering citizens with a high level of safety within an area of freedom, security and justice.

A Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions was issued for creating a **Safer**

²³⁰ Article 29: Without prejudice to the powers of the European Community, the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia.

That objective shall be achieved by preventing and combating crime, organised or otherwise, in particular terrorism, trafficking in persons and offences against children, illicit drug trafficking and illicit arms trafficking, corruption and fraud, through:

— closer cooperation between police forces, customs authorities and other competent authorities in the Member States, both directly and through the European Police Office (Europol), in accordance with the provisions of Articles 30 and 32;

— closer cooperation between judicial and other competent authorities of the Member States in accordance with the provisions of Articles 31(a) to (d) and 32;

— approximation, where necessary, of rules on criminal matters in the Member States, in accordance with the provisions of Article 31(e).

Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime (Annex 37).²³¹

The Communication was a first attempt by the European Parliament to present a comprehensive policy statement on the issue of computer related crime, which was launched by public debate. The Communication discussed the need for initiative in the context of the broader Information Society and Article 29 objectives for improving the security of information infrastructures, in accordance with commitments of the EU to respect fundamental human rights.

The Communication outlined four key conditions to be observed: (1) Adoption of adequate substantive and procedural legislative provisions was essential to deal with both domestic and transnational criminal activities. (2) A sufficient number of well-trained and equipped law enforcement personnel is imperative for the enforcement of new legislative procedures. (3) The improvement of the co-operation between all the actors concerned, users and consumers, industry and law enforcement agencies and (4) the necessity for ongoing industry and community-led initiatives was important if online challenges were to be meant at EU level.

The Communication described five different types of threats to information systems. One concerned unauthorised access to information systems. This includes the notion of "hacking".

Disruption of information systems is another. Different ways exist to disrupt information systems through malicious attacks. One of the best-known ways to deny or degrade the services offered by the Internet is known as a "denial of service" attack (DoS). Also, execution of malicious software that modifies or destroys data was identified as a serious threat. The most notorious type of malicious software is the virus. The Communication noted that interception of communications and malicious misrepresentation also constituted aggravated menaces. These threats were considered and taken into account in a Council Framework Decision on attacks against information systems, which had been discussed previously.

Two other documents, a Communication²³² from the Commission **Preventing fraud and counterfeiting of non-cash means of payment** and a Proposal²³³ for a Council Framework Decision on the **European arrest warrant and the surrender procedures** (Annex 38) between the Member States were issued.

These two proposals are part of a response by the Commission to the threat of a terrorist attack against vital information systems within the EU. It supplements the Commission's proposals to replace extradition within the European Union with a European Arrest Warrant and to approximate

²³¹ 26/01/2001

²³² 9.2.2001

²³³ 19.9.2001

laws on terrorism, on which political agreement was reached at the Laeken European Council meeting held on 14/15 December 2001.

Council of Europe

However in June 1999, a Common Position was adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cybercrime held in the Council of Europe which resulted in the signature of the **Convention on Cybercrime 2001**.

The Convention on Cybercrime's Articles 2 – 10 look to the main offences as laid down by the Convention. These are classed under four groups, which are offences against (1) confidentiality, integrity and availability of computer data and systems; (2) computer-related offences; (3) content-related offences; and (4) offences related to infringements of copyright and related rights.

The Convention uses technologically neutral language, so that offences may be applied to future technological developments in ICTs. Criminal liability only applies where the acts are committed intentionally, understood as “willfully” or “knowingly”, although this is left to national authorities to interpret. The offence must also have been committed without right, meaning without proper authorization. This safeguard is added because the purpose of the Convention is not to criminalize legitimate and common operating and commercial practices.

Chapter two contains the provisions of procedural law which apply to any criminal offence committed by means of a computer system and to the collection of evidence in electronic form. The provisions also contain expedited preservation of stored computer data, production orders, search and seizure orders and real-time collection.

Chapter three includes principles relating to international cooperation such as extradition and mutual assistance regarding investigative powers, provisional measures, as well as an assistance network between participating countries open 24 hours a day and 7 days a week.

The Convention addresses new types of fraud which are being committed, and false documents which are easily replicated to appear like authentic data. Price-tag frauds, online auction fraud, such as shell bidding whereby a seller and a conspirator drive up the price of an item and force unknowing bidders to raise their prices, have become notorious practices in the online world.

Fraudulent online business practices occur all the time on the Internet. The difficulty of determining the authenticity of an individual or entity is made even greater as contact is often not physical and therefore trust is harder to establish online. The development of effective user authentication technologies can provide a solution to this problem. Frauds such as the West African advance fee scam has moved from traditional paper-based mail, to electronic mail, enabling them to reach an

almost unlimited number of people at virtually no cost. The true identity of the sender is easier to disguise as well as the original supporting documentation which cannot be checked for authenticity.

FRAUD

The United States

On the other side of the Atlantic, the US Federal Government has quite a few traditional statutes relating to fraud and forgery. The **Wire Fraud**²³⁴ statute criminalizes the use of interstate and international wire communication (e.g., fax, e-mail, accessing website) in furtherance of scheme to defraud. The **Mail Fraud**²³⁵ statutes cover the use or causing use of mails in furtherance of a scheme to defraud. Under the **Financial Institution Fraud** (Annex 39)²³⁶ legislation, a person knowingly executing, or attempting to execute a scheme or artifice to defraud financial institution, or to obtain money, funds, etc. under financial institution's custody by means of false or fraudulent pretences, representations, or promises is also criminalized.²³⁷

In *United States v. Yip*²³⁸, individuals stole identifying and other data from their employer, and then used the data to open PayPal accounts and fund those accounts by direct transfers from victims' bank accounts. The defendants were found guilty of Financial Institution Fraud.²³⁹

Under subsection 1209(a)(2) of the **Access Device Fraud** (Annex 39)²⁴⁰, it is illegal to, knowingly and with intent to defraud, traffic in or use one or more unauthorized access devices (e.g., access devices obtained with intent to defraud) during any 1-year period, and by such conduct obtaining anything of value aggregating \$1,000 or more during that period. Possession of over 15 unauthorized access devices, with knowledge and intent to defraud, is also criminalized under subsection 1029(a)(3). Additionally, under 1029(a)(5), effecting transactions with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than \$1,000, coupled with knowledge and intent to defraud also constitutes a criminal offence. Under 1029(a)(10) activities performed without authorization of a credit card system or member or its agent, knowingly and with intent to defraud, which cause or arrange for another person to present to member or its agent, for

²³⁴ 18 U.S.C. 1343

²³⁵ 18 U.S.C. 1341

²³⁶ 18 U.S.C. 1344

²³⁷ Cybercrime law: A Global Survey of Cybercrime legislation, Chief Judge Stein Schjolberg,

<http://www.cybercrimelaw.net/index.html>

²³⁸ *S.D.N.Y. 2003*

²³⁹ Asian School of Cyberlaws, Cybercrime Cases: Emerging Jurisprudence,

http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm

²⁴⁰ 18 U.S.C. 1029

payment, 1 or more items of evidence or records of transactions made by an access device will also constitute a criminal offence.

The **Computer Fraud and Abuse**²⁴¹ statute effectively covers intentionally accessing computers without authorization or exceeding authorization, and thereby obtaining information from any protected computer if that conduct involved interstate or foreign communication.²⁴² Knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining anything of value constitutes an offence.²⁴³ Exception to this offence is only in the case where the object of fraud and thing obtained consists only in the use of a computer and the value of such use is not more than \$5,000 in any 1-year period.

United Kingdom

Similar legislation exists in the UK under the **Computer Misuse Act** of 1990. Under section 3, an act, which causes unauthorized modification of the contents of any computer, constitutes an offence. The requisite knowledge, which is knowledge that access is not authorised and intent, are necessary elements for the offence. This includes impairment of the operation of a computer, prevention or hindrance to access or impairment of reliability to any program or data held on the computer. This would effectively criminalize the distribution of viruses and similar programs on the Internet.

People's Republic of China

The criminal law of the People's Republic of China²⁴⁴ criminalizes any person who deliberately creates and propagates computer viruses and other programs, which sabotage the normal operation of the computer system, and causes grave consequences. Creation and propagation of viruses and other types of malware such as Trojans, logic bombs and worms is explicitly prohibited. It is similar to the CMA and although it does not specifically mention viruses, it does make unauthorized access and unauthorised modification of computer material criminal offences.²⁴⁵ It is

²⁴¹ 18 U.S.C. 1030

²⁴² Section 1030(a)(2)(C)

²⁴³ Section 1030(a)(4)

²⁴⁴ Article 286. Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment. Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph. Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.

Article 287. Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

²⁴⁵ Section 3 : Unauthorised modification of computer material.

3.—(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

irrelevant whether the result of the conduct temporary or permanent. A prison term or fine can be incurred by anyone committing these offences. The CMA looks more to the consequences that propagation of any type of program which modifies data in any way will create. This ensures that when new programs are created, which are not specifically viruses, the CMA will capture these and other similar types of programs if the consequences intended by these programs fulfil the stated conditions of modification and impairment of computer data and systems without authorisation. The Chinese criminal law also incorporates a detailed yet broad definition of consequences affected by viruses which are criminalized. This includes alteration, deletion, addition and interference with computer information systems, causing abnormal operations of the systems and grave consequences. More specifically, it expressly prohibits the creation of viruses and other programs, which sabotage the normal operation of a computer. Under the CMA, modification becomes an offence if such action effectively hinders or impairs functioning and reliability. Similarly, under the Chinese law, any modification which causes grave consequences constitutes an offence. In both cases, even a harmless virus like Netsky.D released in March 2004 would come under unauthorised access, since the virus effectively copied and sent itself to all email addresses contained on the infected machine.

Century old crimes like fraud and forgery have evolved with their environment and are fully operative on the online world. The offences relating to computers concern the input, alteration, deletion and suppression of computer data. Regarding forgery, this results in the authentication of false data. Under Article 7 of the Council of Europe's Convention, any modification, variation, partial change, removal of data from a data medium, holding back and concealment of data constitutes a criminal offence. Such acts include phishing, which are bogus websites of established companies, the assumption of false identification in emails, and the posting of false information on bulletin boards.

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

As with its traditional notion, computer-related fraud results in loss of property to another through the input, alteration, deletion and suppression of computer data, as well as any interference with the functioning of a computer system, with the dishonest intent of procuring without right an economic benefit. The aim of such a provision is to “*criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property*”.

One major type of fraud identified by Judge Schjolberg in his report for the WSIS²⁴⁶ Thematic Meeting on Cybersecurity which took place at ITU headquarters in Geneva in June 2005, is the online securities and stock fraud. People are using the Internet to artificially inflate the market value of stocks by creating demand for less traded, low priced stocks.²⁴⁷

Australia

One such example is *Australian Securities and Investments Commission v Steven George Hourmouzis*. The defendant was a shareholder in an American company. With the help of an accomplice, he sent out between 6 and 7 million emails to US and Australian addresses, encouraging the purchase of shares in which the defendant was a shareholder. The volume of share trading increased ten fold after the release of the false information, and the defendant sold off his shares at a profit. The company eventually denied statements made in the various communications and halted trading but not until the price of the shares had doubled. The Australian Securities and Investments Commission (ASIC) filed 19 criminal charges against the accused who pleaded guilty to disseminating false and materially misleading information likely to induce the purchase of securities and to the interference and obstruction of the lawful use of a computer.

Another case can be found in the US, in *Securities and Exchange Commission v World Financial & Investment Co., Inc. and Victor M. Wilson*. Acting through World Financial, the accused, Wilson, raised approximately \$1.2 million from hundreds of investors in the United States and Caribbean from March 1997 through April 1998. The money was invested in a program promoted by Credit Bank International Co. which was purportedly chartered in the "Dominion of Melchizedek." The Dominion of Melchizedek, a non-existent country, has a website promoting itself as a sovereign entity. Wilson solicited U.S. investors by falsely promising returns of over 300% and directed funds to bank accounts controlled by the supposed "ambassador at large" of the Dominion of Melchizedek. Without admitting or denying the allegations made against them, Wilson and World Financial consented to final judgments that permanently enjoined them from committing future violations of Sections 5(a), 5(c), 17(a) of the Securities Act of 1933, Section 10(b) of the Securities Exchange Act of 1934, and Rule 10b-5 there under. The final judgments required Wilson and

²⁴⁶ World Summit on the Information Society

²⁴⁷ Moss tingrett, Moss District Court, The Legal Framework – Unauthorised Access to Computer Systems, Penal Legislation in 44 countries, Judge Stein Schjolberg, April 7, 2003

World Financial to payback gains and interest totalling \$175,000 as well as pay civil penalties. Wilson was additionally barred from associating with any investment advisor.

Online funds transfer is another growing method of fraud that is facilitated on the Internet. Insiders may move funds electronically by sending instructions via email. In 2001, two Indian computer trainers were arrested for allegedly trying to hack into the computers of the State Bank of India, India's biggest commercial bank, and other state agencies. The suspects allegedly sent emails in the name of Microsoft and Videsh Sanchar Nigam, India's monopoly overseas phone service provider, containing a file named Speed.exe. When opened, it sent emails back to the accused giving them passwords and other data. The arrest is the first under the nation's Information Technology Act, which came into force in October 2000. Under the law, anyone found guilty of hacking can face up to three years in jail and US\$4,300 (200,000 rupees) in fines.

However, the lack of experience of the police and the judiciary in this case hindered them from prosecuting the accused, and they were released on bail days after their arrest. The lack of computer equipment in police stations prevents them from collecting electronic evidence and therefore the Information technology Act has not so far been an effective tool in the hands of enforcement authorities. The law becomes useless if proper infrastructure and materials are not available to enforcement authorities.

PHISHING

Phishing is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of social engineering attack. Pharming is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect that website's traffic to another web site. DNS servers are the machines responsible for resolving Internet names into their real addresses. If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN number or account number.²⁴⁸

Direct financial losses from phishing attacks cost U.S. financial services firms about \$1.2 billion in 2003. Any criminal scheme in which digital communications play a significant role in acquiring multiple victims' identifying or personal financial data by deception, and transferring or

²⁴⁸ Anti-Phishing Working Group, What is Phishing & Pharming?, <http://antiphishing.org/>

transmitting multiple victims' data via the Internet for criminal use is commonly known as phishing. Several legislative instruments exist criminalizing fraud.²⁴⁹

Phishing can be classed generally into three different categories. The most common is the dragnet method. E-mails with falsified corporate identification direct a large class of people to websites with similarly falsified identification. The specific prospective victim is not identified in advance, but the false information is conveyed indiscriminately to trigger immediate response.

One example of the dragnet method can be seen in the case *United States v. Forcellina*²⁵⁰ where a husband accessed chat rooms, used a device to capture screen names of chat room participants and then sent e-mails pretending to be the ISP requiring correct billing information, including current credit-card number. He used the credit-card numbers and other personal data to arrange for wire transfers of funds via Western Union. The husband and his wife were charged with conspiracy to commit access device fraud.

A similar case took place in *United States v. Hill*²⁵¹ where the defendant operated AOL and PayPal phishing schemes to fraudulently obtain credit-card numbers to purchase goods and services costing more than \$47,000. The defendant pleaded guilty in February 2004 to possession and use of access devices and was sentenced to 46 months imprisonment.

In *United States v. Carr*²⁵², Helen Carr was accused of sending fake e-mail messages to AOL customers in United States and several foreign countries. The emails advised the customers that they must update their credit card and personal information on file with AOL to maintain their accounts. She was found guilty of conspiracy to possess unauthorized access devices and sentenced in January 2004 to 46 months imprisonment.

*United States v. Guevara*²⁵³ concerned a young man who created false e-mail accounts with Hotmail and unauthorized website with the address www.msnbilling.com through Yahoo!. He then sent MSN customers e-mail messages, purporting to come from MSN, that directed customers to the fraudulent website and asked them to verify their accounts by providing name, MSN account, and credit card data. The website automatically forwarded each customer's data to one of the defendant's false Hotmail accounts. He pleaded guilty in September 2003 to wire fraud and was sentenced to 5 years probation and 6 months home confinement.

The rod-and-reel method targets prospective victims with which initial contact has already been made. The victims are thus defined in advance and false information conveyed to trigger responses.

²⁴⁹ Phishing: A Growing Threat to Financial Institutions and E-Commerce by Frederick W. Stakelbeck, Jr., Training and Development Coordinator, December 2004, <http://www.phil.frb.org/src/srcinsights/srcinsights/Phishing%20-%20Dec%2004.pdf>

²⁵⁰ D. Conn., sentenced Apr. 30 and June 18, 2004

²⁵¹ SD Tex., sentenced May 2004

²⁵² ED Va. 2003

²⁵³ WD Wash. 2003

In *United States v. Gebrezihir*²⁵⁴, the accused was allegedly involved in a scheme to send phoney letters on bank letterhead, along with altered or counterfeit IRS forms to victims, generally foreign nationals living abroad with bank accounts in the United States.

Some of the altered or counterfeit forms appeared similar to actual IRS forms that are sent to non-resident aliens who maintain U.S. bank accounts. The fraudulent bank letter instructed victims to fill out fraudulent IRS form, which required personal information concerning the victim and victim's bank account, and then to fax the completed form, ostensibly to the IRS or to the bank fax numbers provided. The numbers were in fact Internet-based fax numbers that convert all incoming faxes to e-mail attachments and then forward these attachments to free e-mail accounts. Wire transfer instructions were then sent to banks and, in many instances, large amounts of money were transferred from victims' accounts. The overall investigation by the IRS has identified more than \$700,000 in losses.

Cases coming from the Eastern European block are also quite notorious. In 2003, the Romanian General Directorate for Combating Organized Crime, in cooperation with Secret Service, arrested a subject in Alba Julia, Romania²⁵⁵. The individual forwarded spoofed e-mails resembling actual auction webpage to the attention of unsuccessful bidders in an online auction. On the spoofed page, the subject advised victims of availability of similar items for a better price. However, upon visiting the "sale" page, victims were asked for personal information including their name, bank account numbers and passwords. Once these were filled in, the victims were then advised that they had "won" the spoofed auction and agreed to send money to the subject through a spoofed escrow site created by the accused. The scheme resulted in nearly \$500,000 in on-line losses.

The Lobsterpot method involves the creation of websites similar to legitimate corporate websites which narrowly define a specific class of victims. There is a smaller class of prospective victims which are identified in advance.

A good example of this method can be seen in the case of *United States v. Kalin*²⁵⁶. The defendant Nevada resident, allegedly registered four websites with domain names deceptively similar to website operated by DealerTrack, Inc. DealerTrack provides services via the Internet to auto dealerships located throughout the United States, including dealers' ordering credit reports on prospective automobile buyers. The defendant's website was designed to be practically identical to main page of DealerTrack. He then allegedly got a number of dealership employees mistakenly to enter usernames and passwords at his sites and consequently managed to obtain unauthorized access to DealerTrack for personal data.

²⁵⁴ SDNY 2003

²⁵⁵ Operation Cybersweep, US Department of Justice, <http://www.fbi.gov/cyber/cysweep/cysweep1.htm>

²⁵⁶ DNJ, Nov. 2003

In April 2004, the UK's National High-Tech Crime Unit (NHTCU) arrested a 21-year-old British national for "copycat" phishing scheme involving online bank.²⁵⁷ This was reportedly the first in the United Kingdom. In May 2004, NHTCU arrested 12 Eastern European nationals suspected of laundering money from "phished" bank accounts. British police acted to end these threats by making one of the largest arrests of phishers to date. The individuals were accused of stealing hundreds of thousands of pounds from British bank accounts and depositing them into Russian accounts.

More recently, in June 2005, the NHTCU arrested a US and a UK citizen who, together, masterminded a £6.5m fraud network stretching from ex-KGB agents in Russia to hackers in America. Starting in Russia, the fraudulent network recruited individuals to send spoof e-mails in an attempt to coax people's credit card details, under the guise of updating accounts or fixing a payment error.²⁵⁸ The individuals then bombarded global mail accounts with their phishing e-mails, after handing their catch of credit card data to Harvard and Elwood, in return for 60 per cent of any profits made. The first people in Britain to be convicted of committing fraud by using credit card numbers distributed over the Internet, Douglas Harvard and Lee Elwood, pleaded guilty at Leeds Crown Court in early July 2005.²⁵⁹

In *Germany*, Postbank and Deutsche Bank AG²⁶⁰, were victims of phishing attacks in August 2004. In both cases, the e-mails asked that bank customers impart personal identification and transaction numbers to resolve non-existent account problems. The attacks supposedly originated in the Far East and Russia. In Hong Kong, customers of the Hong Kong and Shanghai Banking Corporation²⁶¹ were targeted by a syndicate purporting to be a Hong Kong bank. From September 17, 2004 through October 6, 2004, bank customers received phishing e-mails asking them to click on an embedded hyperlink connected to a fraudulent web site. Eleven individuals ranging in ages from 21 to 58 were arrested in this case.²⁶²

IDENTITY THEFT

The US has a statute covering **Identity Theft** (Annex 39)²⁶³. Identity theft is defined as knowingly using, transferring, or possessing another (real) person's "means of identification". This includes

²⁵⁷ National Hi-Tech Crime Unit, http://www.nhtcu.org/nqcontent.cfm?a_id=12261

²⁵⁸ BBC News [Phishing pair jailed for ID fraud](http://news.bbc.co.uk/2/hi/uk_news/4628213.stm) http://news.bbc.co.uk/2/hi/uk_news/4628213.stm

²⁵⁹ BBC News [Phishing pair jailed for ID fraud](http://news.bbc.co.uk/2/hi/uk_news/4628213.stm) http://news.bbc.co.uk/2/hi/uk_news/4628213.stm

²⁶⁰ [Big German banks hit by phishing attacks](http://www.computerworld.com/industrytopics/financial/story/0,10801,95429,00.html) by John Blau AUGUST 23, 2004

<http://www.computerworld.com/industrytopics/financial/story/0,10801,95429,00.html>

²⁶¹ [HK\\$660,000 Phishing Scam](http://www.spamfo.co.uk/component/option,com_content/task,view/id,139/Itemid,2/) by Mike Carter, Sunday, 17 October 2004

http://www.spamfo.co.uk/component/option,com_content/task,view/id,139/Itemid,2/

²⁶² EurActiv, [Finance Fraud](http://www.euractiv.com/Article?tcaturi=tc:29-140752-16&type=LinksDossier), 9 June 2005, <http://www.euractiv.com/Article?tcaturi=tc:29-140752-16&type=LinksDossier>

²⁶³ 18 U.S.C. 1028(a)(7)

name, birthday, driver's license, passport number, unique biometric data or access device (e.g., credit-card or financial account number) with intent to commit or aid and abet, or in connection with, any unlawful activity that constitutes a federal violation or state or local felony.

The defendant in the case of *United States v. Butcher*²⁶⁴ allegedly applied for 10 credit card accounts using the identifier information of another person, including her name, Social Security account number and date of birth, without authorization.

Similarly, in *United States v. Christensen*²⁶⁵, the defendant used more than 50 different identities of prison inmates serving long sentences to obtain more than \$313,000 in student loans. The defendant pleaded guilty to charges under the Act.

The **Aggravated Identity Theft**²⁶⁶ Act was signed into law on July 15, 2004. Aggravated identity theft concerns knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person, during and in relation to any felony violation enumerated in subsection 1028A(c) [including numerous fraud offences]. Conviction entails, in addition to the punishment provided for such felony, sentence of 2 years imprisonment and 5 years in terrorism-related cases. The sentence must be consecutive with the sentence for the underlying felony.²⁶⁷

In Japan, one individual opened bank accounts under false names using forged health insurance certificates and advertised them for sale on the Internet, to customers using the accounts to perpetrate fraud and other crimes. He opened some 50 bank accounts with an accomplice. They were eventually arrested in 1999 for alleged forgery and use of private documents.²⁶⁸

INSIDER FRAUD

Many financial-oriented crimes are taking place in the online world. Fraud such as procurement fraud takes advantage of purchasing activities online since tenders can be disseminated widely and documents exchanged electronically. In Australia, for example, a sub-contractor to a local council gained access to its database of tendering information and used this to secure numerous contracts. Many other government sectors are affected as well, such as benefits and welfare programs. Another Australian incident concerned the Electronic Benefits Transfer system being compromised. The system issues cards with which beneficiaries are able to take cash out of an ATM. Internal employees issued cards in fictitious names and used them to obtain cash for themselves.

²⁶⁴ 53 MJ 711, 712, 714 (AF Ct. Crim. App. 2000)

²⁶⁵ 403 F.3d 1006 (8th Cir. 2005)

²⁶⁶ 18 U.S.C. 1028A

²⁶⁷ Avoid Identity Theft, Identity Theft Legislation, <http://www.avoid-identity-theft-guide.com/identitytheftlegislation/>

²⁶⁸ The Japan Times: Sept. 13, 1999 <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn19990913a7.htm>

Any electronic monetary claims or compensations can easily be abused by internal elements if strong security from inside government agencies, organisations or institutions is not in place. Health, welfare and taxation systems, among many other government agencies are susceptible of internal fraud, which can sometimes take much longer to detect. Non-monetary motivated fraud also takes place in government agencies. One example is of four employees of the Australian Department of Child, Youth and Family Services were dismissed for gaining access to pornographic material. It is clear that the facility with which traditional acts can be perpetrated online will take longer to be noticed and tracked down. This can also affect private sectors like telecommunications, where theft of services and non-provision of services are recognized crimes. In *Federal Trade Commission v Audiotex Connection Inc*²⁶⁹, software available on the internet was downloaded unknowingly when a user clicked on an erotic photograph at a designated website. The software took control of the users modem, cut off the ISP and dialled a number in the former Soviet Republic of Moldova. The line would remain open until the computer was turned off. The charges were shared between the fraudster and the Moldovan telecommunications company. The US Federal Trade Commission eventually detected the fraud through regular surveillance of customer telephone accounts.

Credit card theft has also taken huge proportions on the online world. This type of information is threatened both on the inside, by employees, and externally through attacks.

In *R. v Governor of Brixton Prison, Ex parte Levin*²⁷⁰. *In re Levin*²⁷¹, a group of Russian hackers managed to steal approximately \$10.7 million from various Citibank customer's accounts by manipulating the system's computerized transfer funds. After protracted legal proceedings which went to the House of Lords, the defendant was extradited to stand trial before the Federal District Court in New York's Southern District. On 24 February 1998, he pleaded guilty to conspiracy to defraud and was sentenced to thirty-six months' imprisonment and ordered to pay Citibank US\$240,015 in restitution. Citibank was able to recover all but \$240,000 of the \$10.7 million worth of illegally transferred funds. None of the bank's depositors lost money and since the fraud was discovered and Citibank recovered the money from the fraudster. As a consequence, Citibank required customers to use an electronic password generator for every transfer of funds. The consequences for Citibank's business reputation were, however, considerable.

Outsourcing risks for data protection, consumer fraud, theft of financial information such as credit cards, online extortion are among many other types of frauds that are committed online, and as new technologies and processes are developed, new types of fraud will emerge. With society rapidly

²⁶⁹ *E.D.N.Y. Filed 13 February 1997*

²⁷⁰ [1996] 3 WLR 657

²⁷¹ House of Lords, 19 June 1997

sailing aboard the online world into new and unknown waters, it is usually only after a fraud is committed and detected that realization of a problem occurs and action is taken, often too late. The goal should be not to restrain this evolution but to ensure security and safety on board in order to weather future icebergs.

In an article for Wired News, dated January 2005, Manu Joseph clearly showed that although a country might have sufficiently adequate laws in place to deal with cybercrimes, the authorities in charge of investigating such crimes must imperatively be educated and trained in the field for enforcement of the law and protection is to be efficiently undertaken. *"The cop who checks your car license does not own a car,"* said Raghu Raman, who heads an information security firm called Mahindra Special Services Group in India. *"The passport official who checks your passport does not go abroad. The cop to whom you go to register a credit card misuse does not own a credit card. If a cop is in no position to own a computer, how can he fight cybercrime? The field cop (and) the beat constable live in another world."*²⁷²

Japan

The **Japanese penal code** (Annex 40) has adopted measures against computer crimes, which took effect from February 2000.²⁷³ Lawmakers tried to be as complete as possible in adapting traditional crimes to the online environment.

Section 7-2 of the penal code defines the term electronic-magnetic records as a record [data] or records which are produced by electronic, magnetic or other unrecognisable measures, and which are intended to or able to be used to perform information processing in computer systems. This definition can be considered to be technology neutral since it provides for future technologies to be covered by the law.

Chapter 17 of the penal code deals with forgery of documents. More precisely, section 161-2 criminalizes the unlawful production of electronic-magnetic records. The prerequisite of intention and knowledge are the same as can be found in European legislation. False reproduction of legal rights and duties belonging to others, which are intended for use in business transactions, is illegal. Forgery of documents undertaken by a State or public office employee incurs a penalty double that of a non-state or public officer. This section ensures a safeguard against corruption at the State and public level. Both production and use of such documents are penalized.

Chapter 36 of the Japanese Penal Code concerns interference with credit and transactions. Section 234-2 criminalizes interference in business transactions by the use of computer systems. Any

²⁷² Wired News, [India's Odd Couple: Cops & Tech](http://www.wired.com/news/technology/0,1282,66123,00.html?tw=wn_story_related), Manu Joseph, January 5, 2005, http://www.wired.com/news/technology/0,1282,66123,00.html?tw=wn_story_related

²⁷³ Privacy International, Country Reports, Japan, <http://www.privacyinternational.org/survey/phr2000/countrieshp.html>

interference with the regular execution of a valid performance of a computer system which is being used in business transactions, or causes executions which are contrary to the proper use or purpose of the computer system constitutes a criminal offence. This includes activities such as the destruction of the system or electronic-magnetic records used or intended for use by the system, through the introduction of false information or incorrect instructions, or by other similar means. Interference with the business transaction of others through the use of a computer system effectively guarantees the protection of e-commerce related activities.

Under Chapter 36, concerning theft and burglary, section 245 categorizes electricity as property, thus making theft of data or services provided online illegal. A subtle addition, but one which might solve many problems related to theft of intangible property.

Chapter 37 looks to fraud and threatening. Section 246-2 criminalizes computer fraud specifically, stipulating that any person who intentionally or knowingly obtains unlawful profits for himself or others by introducing false information or incorrect instructions to a computer system which is being used or intended to be used in third party business transactions, by introducing false electronic-magnetic records in any business transaction will be liable to a prison term. A fine is not even possible. The only sentence which can be handed down is a prison term. Section 250 states that any person who attempts computer fraud or threatens to commit such fraud will be similarly punishable.

Chapter 40 deals with damage and concealment of electronic-magnetic records. Section 258 and 259 deal with the destruction of official and private records respectively. A minimum prison sentence of 3 months is however set for destruction of official records, once again underlining the element of deterrence at state level.

The Penal code also defines jurisdictional boundaries in section 1, clearly stipulating that any crime committed inside Japanese territory, Japanese aircrafts and ships is punishable. Any crimes falling under section 161-2 will be covered by the Japanese jurisdiction even if they are committed outside Japanese territory.

Japanese police also arrested four people for fraudulently hacking into an on-line bank account and transferring 360,000 yen to another account. This conduct was also a violation of the Anti-Hacking Law 2003. Another party arrested for violating the Anti-Hacking Law involved a person who accessed a university server more than 100 times reading email and closing down its bulletin board. The employee had been transferred to a less desirable position.²⁷⁴

²⁷⁴ CYBER-CRIME/CYBER-REGULATION
http://www.japanlaw.info/law2004/JAPAN_LAW_2004_CYBER_CRIME_CYBER_REGULATION.html

United Nations

The latest UN recommendations (Annex 41) on fighting cybercrime as published by the Computer Crime Research Center in May 2005, workshop 6 recommended that countries consider several important elements for fighting cybercrime. A broad focus should be kept on the secure functioning of a cyber-economy optimising business confidence and individual privacy, as well as adopting strategies to promote and protect the innovation and wealth-creating potential and opportunities of information and computing technologies, including early warning and response mechanisms in case of cyberattacks. The challenge of creating a global culture of cybersecurity, addressing the needs of even the weakest links in the chain is still unmet and prevention and prosecution of computer-related crimes is just the first step.

The recommendations also stressed the importance of international cooperation at all levels, with the UN leading the way for intergovernmental activities to ensure the functioning and protection of cyberspace so that it is not abused or exploited by criminals or terrorists. The UN can be instrumental in combating cybercrime and establishing procedures for international collaboration, with a view to averting and mitigating the negative impact of cybercrime on critical infrastructure, sustainable development, protection of privacy, e-commerce, banking and trade. Additionally, the recommendations encourage all states to update their criminal law in order to adequately address the specific nature of cybercrime. Review of traditional legislature in light of present and future technologies is necessary so that crimes such as unauthorized access to computers or computer networks can be effectively prosecuted. The recommendations add that such updating should also include procedural laws (for tracing communications, for example) and laws, agreements or arrangements on mutual legal assistance (for rapid preservation of data, for example). States are encouraged to look at the provisions of the Council of Europe Convention on Cybercrime.

Finally, the recommendations also urge governments, private sectors and non-governmental organizations to work together to bridge the digital divide and raise public awareness about the risks of cybercrime by introducing suitable countermeasures, and improving the capacity of criminal justice professionals, including law enforcement personnel, prosecutors and judges. National judicial administrations and legal educative institutions including comprehensive criteria on computer related crime in their teaching schedules.

In order to ensure efficiency and effectiveness in the battle against cybercrime, policies should be evidence-based and subject to rigorous evaluation. It is vital therefore that concerted and coordinated efforts be made at a supranational level to establish a funding mechanisms to facilitate

practical research and in order to curb new types of cybercrime and that the results be made widely available to the public.

CONCLUSION

With all new wonders, come new worries. The Internet is no exception. In just over a decade, this technological miracle has brought societies the world over closer together than in the whole history of international relations. Unfortunately, this has meant that disruption of its infrastructure will have a global effect. The Internet can only ever be as secure as its weakest link. In order to strengthen the overall infrastructure, efforts by each country must be made at a supranational level in an attempt to cooperate and coordinate with each other so as to come to harmonised terms on matters regarding security. In light of the tremendous growth of electronic commerce, the potential for many developing countries is great. Minimum physical infrastructure is required, and thus capital investment, which previously would have been used in construction and production on physical locations, can be used for launching and securing online business.

Credibility in a country's e-commerce activities heavily relies on the validity and authenticity of electronic contractual relationships. If legislative enforcement cannot be guaranteed, then contractual relations will be undermined. Electronic contracts and electronic evidence have become an accepted format in Courts and recognised by Governments in many developed countries. With the use of encryption technologies, electronic signatures have become binding on contractual documents. Cryptographic techniques such as the Public Key Infrastructure has become one of the most reliable technologies up to date for authenticating individuals. This form of electronic signature has become internationally recognised, with involvement by the United Nations with the UNCITRAL Model Law on Electronic Signatures of 2001. Encryption technologies also help secure confidentiality of communication, for contractual and non-contractual communication alike.

Privacy however has become another matter. Although encryption technologies may be applied to protect users' privacy, not all data about a user will be under his control. Collection of data by public and commercial entities remains widely accepted but calls for protection of the data have reached listening ears in the European Union. Data protection directives have been pronounced at Union level, and Member States have enacted laws to protect users' data online. However, such laws cannot reach further than their own jurisdiction, and as long as users can access websites and impart personal identifying information to a site in a country where no data protection laws exist for electronic communications, then their own data protection laws cannot protect that information without a mutual recognition and cooperation treaty between the two countries.

Privacy has also been threatened by the ever growing problem of unsolicited commercial emails, otherwise known as spam. Spam represents a significant challenge to users, Internet service providers, states and legal systems worldwide. The cost of spam is significant and growing, and its increasing volume threatens to destroy the utility of electronic communications.²⁷⁵ During the ITU WSIS Thematic Meeting on Countering Spam in July 2004, the Chairman's Report emphasised the importance of a comprehensive approach to solving the problem of spam and made legal governance one of the necessary means. During the 2005 ITU Thematic Meeting on Cybersecurity in July 2005, a comparative analysis of spam laws was undertaken in order to optimise the pursuit for a model law in this area. It is suggested in this analysis that an alignment and conformity of legal rules can improve enforcer's ability to operate, as spammers do, across jurisdictional borders.

Additionally, it is suggested that the creation of a model law would reduce the cost and challenges for legal systems that have not yet addressed spam issues, stating that these countries could enact and implement the law with confidence that it approaches a set of best practices in this area. The analysis however underlines that a model law is not an instant solution to the spam problem. Cleaning up spam is a question of resources, enforcement and the effective integration of anti-spam laws with existing technology, market and norms-based approaches. Regulators will have to work closely with technical experts to track spammers down and collect electronic evidence of violations. It is not just a question of implementation of anti-spam laws, but also of effective enforcement. This problem has become increasingly important over the past few years, as a significant percentage of spam promotes some type of fraud against the recipient, from phishing scams to viruses used for denial of service attacks, including illegal financial schemes and offers for products of dubious quality or legality.²⁷⁶

Cybercrime has also taken on a global scale, with criminals basing themselves in countries with little or no legislation against cybercrime. However, with international instruments such as the Council of Europe's Convention on Cybercrime 2001, ratification of such a treaty by countries could prove extremely valuable in fighting cybercrime at an international level. Although many countries have signed, only a few have ratified it and the legislative and enforcement authorities in many countries are slow on the uptake. Countries should be aware however that with the current pace of technological developments, the international dimension of cybercrime, and consequently of cybersecurity, is yet uncharted. The targets of attacks affect the whole of the Internet and although at the moment, the main targets are private companies and individual end-users, it will not be long before attacks on critical infrastructure become common.

²⁷⁵ ITU WSIS Thematic Meeting on Cybersecurity, A Comparative Analysis of Spam Laws: the Quest for a Model Law, Geneva, 28 June – 1 July 2005

²⁷⁶ United States Federal Trade Commission, False Claims in Spam, 2003, <http://ftc.gov/reports/spam/030429spamreport.pdf>

Developing countries are the most concerned with this. Lack of security can and will effectively spoil the benefits of the Internet, both on an economic and governmental scale. Furthermore, failure to ensure adequate minimum security standards will negatively affect the rest of the world, and might even lead to a refusal by other countries to connect with it, thus excluding it from the new world order. It is clear the international cooperation cannot be limited to technological considerations. Law enforcement and national security must also play a determining role. But ensuring security in cyberspace will require an international law enforcement effort. It will also be imperative that countries cooperate with each other, and that real efforts are made to assist developing countries which often lack experience and legal knowledge on this front. It is vital that countries do not underestimate the importance of securing cyberspace if the Internet is to flourish to its full capacity, bestowing its benefits on a global scale.

BIBLIOGRAPHY

I. INTELLECTUAL PROPERTY

COPYRIGHT & DIGITAL RIGHTS MANAGEMENT

International

- Bern Convention & Paris Convention
- WIPO Copyright Treaty 1996
- WIPO Phonograms & Performers Treaty 1996

US

- Title 17 of the United States Code
- Digital Millennium Copyright Act 1998
- No Electronic Theft Act 1997
- Sony-Betamax
- [A&M Records v. Napster](#) 239 F.3d 1004 (9th Cir. 2001)
- US v Elcom Ltd. aka Elcom Co. Ltd. & Dmitry Sklyarov U.S. District Court Northern District of California, May 8, 2002. 203 F.Supp.2d 1111
- Universal v Eric Corey & 2600 Enterprises Inc No. 00-9185 (2d Cir. 2001)
- Mtreo-Glodwyn-Mayer Studios Inc. et al. V Grokster ltd. US District Court, California, [2002], lines 15 – 19

EU

- Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society
- Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programmes, amended by Council Directive 93/98/EEC of 29 October 1993
- EU Copyright/ Rental Right Directive 91/100/EEC
- EU Copyright/ Term of Protection Directive 93/98/EEC

Canada

- The Canadian Copyright Act R.S. 1985, c. C-42

Secondary Sources

- [Digital Music Usage and DRM: Results from a European Consumer Survey](#) by Nicole Dufft, Andreas Stiehler, Danny Vogeley, Thorsten Wichmann, May 24, 2005.
- [Wikipedia: The Free Encyclopedia](http://en.wikipedia.org/). <http://en.wikipedia.org/>

- The UCLA Online Institute for Cyberspace Law and Policy. A&M Records v. Napster: MP3 File Sharing Disputes Continue in the Aftermath of Recent Court Rulings, <http://www.gseis.ucla.edu/iclp/napster.htm>
- Electronic Frontier Foundation: Unintended Consequences: Five Years under the DMCA, September 24, 2003. <http://www.eff.org/>
- Critique of the Proposed UK Implementation of the EU Copyright Directive by Julian T. J. Midgley (jtjm@ukcdr.org), Campaign for Digital Rights: <http://ukcdr.org/issues/eucd/ukimpl/>
- INDICARE: DRM and developing countries by Manon Ress, Washington DC, USA on 29/04/05
- Digital Music Usage and DRM: Results from a European Consumer Survey :The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe by Nicole Dufft, Andreas Stiehler, Danny Vogeley, Thorsten Wichmann, May 24, 2005.
- Canada Declares P2P Downloading Legal December 18, 2003 By [Bill Rosenblatt](#), <http://www.drmwatch.com/legal/article.php/3290471>
- Associated Press: Court Rules Against DVD Copy Preventions, Tuesday April 26, 6:11 pm ET By Mary Maccarthy, Associated Press Writer

TRADEMARK & DOMAIN NAMES

International

- WTO Agreement on Trade-Related Aspects of Intellectual Property Rights
- WIPO “The management of Internet Names and Addresses: Intellectual Property Issues”
- WIPO Internet Domain Name Processes 1999 & 2001
- ICANN Domain Name Dispute Resolution Policy
- Telstra Corporation Limited v. Nuclear Marshmallows Case No. D2000-0003

US

- Anticybersquatting Consumer Protection Act of 1999 (ACPA)
- US Federal Trademark Dilution Act
- Intermatic Inc. v. Dennis Toeppen (pre-ACPA) No. 96 C 1982. United States District Court, N.D. Illinois, Eastern Division. Nov. 26, 1996
- Jack in the Box Inc. v. jackinthebox.org and jackinthebox.net 143 F. Supp. 2d 590, 592 (E.D. Va. 2001)

EU

- EU’s Trademark directive, No. 89/104/Eec

- [EU Regulation 733/2002](#)

UK

- United Kingdom Trade Marks Act, 1994
- Harrods v UK Network Services Limited and Others Chancery Division, 9 December 1996 (unreported)
- BT v One in a Million Ltd, The Times, 2/12/9²⁷⁷ & Marks and Spencer v One in a Million Ltd [1998] unreported 23/7/98 Court of Appeal, 23 July 1998 (unreported)

Secondary Sources

- Anticybersquatting Consumer Protection Act Copyright © 1999-2001 Submerged Ideas, Inc. <http://www.submerged-ideas.com/litigation/anticybersquat.htm>
- Cybersquatting and Trademark Infringement by Monica Kilian, University of Melbourne, E Law – Murdoch University Electronic Journal of Law, Vol 7, No 3 (September 2000)
- WIPO Arbitration and Mediation Center: Administrative Panel Decision <http://arbitrator.wipo.int/domains/decisions/html/2000/d2000-0003.html>
- Nolo Glossary: Domain Name. Legal Information, Books & Software, <http://www.nolo.com/definition.cfm/Term/3E9F8AE7-B46F-40A6-9E737BBFA8FDAE75/alpha/D/>
- FAQ: The Anticybersquatting Consumer Protection Act, by Richard Keyt April 20, 2001. Keyt Law: Business, Internet, E-commerce & Domain Name Law. Domain Name Disputes <http://www.keytlaw.com/urls/acpa.htm#What%20is%20the%20ACPA>
- Trademarks, domain names and patents by M Viljoen, GM du Plessis, G Vivier Beng, Partners at Adams & Adams, Pretoria.

HYPertext LINKING, FRAMING & METATAGGING

US

- Ticketmaster Corp. v. Tickets.com (99-7654)
- The Washington Post, et als. v. TotalNews, Inc., et als [2002] Southern District of New York, Civil Action Number 97-1190
- Futuredontics Inc. v. Applied Anagramic Inc., 1997 46 USPQ 2d 2005 (C.D. Calif. 1997).
- Playboy Enterprises, Inc. v. Calvin Designer Label 985 F.Supp. 2d 1220 (N.D. Cal. 1997)

UK

- *Shetland Times Limited v Dr Jonathan Wills & Another* 1997 F.S.R. (Ct. Sess. O.H.), 24 October 1996

Denmark

- *Danish Newspaper Publisher's Association v. Newsbooster*, Decision of July 5, 2002, Copenhagen Bailiff's Cour

France

- *Havas et Cadre On Line c/ Keljob*, Tribunal de Commerce de Paris, 26 décembre 2000

Secondary Sources

- Internet Ruling: Hypertext Linking does not violate Copyright. Elijah Cocks, Staff Writer. http://www.bc.edu/bc_org/avp/law/st_org/iptf/headlines/content/2000040401.html
- *Netlitigation: Internet Law: News, Suits and Discussions*, by Sugarman, Rogers, Barshak & Cohen, *Linking, Framing and Metatagging*. <http://www.netlitigation.com/netlitigation/cases/shetland.htm>
- Cyberlaw India: To Link or Not to Link-The Judicial View by Shri Pavan Duggal, Cyberlaw Consultant, President Cyberlaws.net, MAC, ICANN <http://www.cyberlaws.net/cyberindia/linking.html>
- Deep links are legal in Germany. Official By [Drew Cullen](#) Published Sunday 20th July 2003 22:52 GMT http://www.theregister.co.uk/2003/07/20/deep_links_are_legal/
- Links & Law - Information about legal aspects of search engines, linking and framing: The German Federal Court of Justice rules on the liability for hyperlinks, Update 18: June 11, 2004 <http://www.linksandlaw.com/news-update18.htm>
- <http://www.virtulaw.com/e-law.htm>, Virtulaw, L.L.C. Copyright © 1999 Virtulaw, L.L.C. All rights reserved. Revised: June 04, 1999.

II. NETWORK SECURITY

AUTHENTICATION

International

- UNCITRAL Model Law on Electronic Signatures (2001)
- Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

EU

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

UK

- Electronic Communications Act 2000 (ECA)
- Electronic Signatures Regulations 2002 (ESR)

US

- Electronic Signatures in Global and National Commerce Act 2000 (E-Sign Act)

Argentina

- The Ley De Firma Digital (Digital Signature Law) was passed by Argentina in 2001.
- Presidential Decree No. 427/98. Signed by President of Argentina April 16, 1998. Digital Signatures Limited to the National Public Sector.
- The Presidential Decree 1023/01 was passed on August 13, 2001 allowing for purchasing by Certification Authorities:
- Resolution 212/98- New Regulation regarding the licensing of Certification December 30, 1998

France

- Case 00-46467, a Decision of the Cour de Cassation, dated 30 April 2003

Germany

- AG Bonn (Decision of 25 October 2001).

Greece

- Court of First Instance in Athens, Decision 1327/2001

Lithuania

- February 20, 2002 Lithuanian Supreme Court in the case Židrūnas Šapalas v. AB “Lietuvos taupomasis bankas”

Sweden

- Swedish Supreme Administrative Court (Case number 2572-2573-2002) 18 December 2002

Secondary Sources

- National Institute of Standards and Technology Computer Security: Recommendation for Key Management – Part 1: General (Glossary of Terms and Acronyms) by Elaine Barker, William Barker, William Burr, William Polk and Miles Smid. NIST Special publication 800-57, April 2005
- Intell recovery: Data Recovery Definition, <http://www.intellirecovery.com/glossary/c.html>
- Wikipedia: The Free Online Encyclopedia

- Electronic Law Journals – JILT 2003 – Public Key Infrastructure, Digital Signatures and Systematic Risk by Jamie Murray, Liverpool John Moores University House of Commons Research Paper 99/92, The Electronic Communications Bill, Bill 4 of 1999-2000, 24 November 1999
- Department of Trade and Industry, Information Security: Guide to the Electronic Communications Act 2000 http://www.dti.gov.uk/industry_files/pdf/622.pdf
- Explanatory Notes to Electronic Communications Act 2000, Chapter 7 <http://www.opsi.gov.uk/acts/en2000/2000en07.htm>
- STATUTES ON COMPANY LAW UPDATE 4 FEBRUARY 2004 Electronic Communications Act 2000 Section 15 <http://www.oup.com/uk/booksites/content/019925947X/12886025/13539537/041eca2000.pdf>
- APPROACHES TO ELECTRONIC SIGNATURES S.C.W.MASON <http://www.pravo.by/leginform/pdf/0105/mason.pdf>
- Study for the European Commission- DG Information Society: The Legal and Market Aspects of Electronic Signatures by Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma & Patrick Van Eecke. Interdisciplinary Centre for Law & information Technology, Katholieke Universiteit Leuven.
- Review of Lithuanian case law on the electronic signatures, Regija Law Firm. www.bakernet.com/ecommerce/lithuania-t7.doc Supra 14
- Baker & McKenzie: E-Law Alert. USA: ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT http://www.bakernet.com/ecommerce/E-SIGN_Act.htm APPROACHES TO ELECTRONIC SIGNATURES S.C.W.MASON
- <http://www.pravo.by/leginform/pdf/0105/mason.pdf>
- IT Landscape in Argentina: Transborder Data Flows, American University of Washington D.C. <http://www.american.edu/carmel/gg7870a/Transborder.htm>

ACCESS CONTROL & COMMUNICATION SECURITY

International

- Council of Europe Convention on Cybercrime 2001

EU

- Proposal for a Council Framework Decision on attacks against information systems 2002

UK

- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (RIPA)
- R v Cropp [Attorney-General's Reference (No. 1 of 1991) [1992] 3 WLR 432]
- R v. Bignall [1997] (Crim LR 53, 1998)
- Denco v. Joinson Employment Appeal Tribunal 14 November [1991] 1 WLR 330
- Regina v Bow Street Magistrates Court Ex parte Allison QB (Times 2nd of June 1998)

US

- Briggs v. State of Maryland 348 Md. 470 (1998) [USA]
- Scott Moulton and Network Installation Computer Services, Inc. v. VC3 Civ. Act. No. 1:00-CV-434-TWT (N.D. Ga. November 6, 2000) [USA]

Australia

- Regan Gerard Gilmour v. Director Of Public Prosecutions (Commonwealth) No. 60488/95 In The Supreme Court Of New South Wales [Australia]
- Director of Public Prosecutions v Murdoch (1993) 1 VR 406 [Australia]

Secondary Sources

- Cole Durham, Brigham Young University, Utah, USA
- Harmonizing National Legal Approaches on Cybercrime by Judge Stein Schjolberg & Amanda M. Hubbard, ITU WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June – 1 July 2005
- Council adopts decision on attacks against information systems 10 March, 2005 Digital Civil Rights in Europe, [EDRI-gram - Number 3.5](#)
<http://www.edri.org/edriagram/number3.5/attacks>
- The Journal Information Systems Committee, Senior Management Briefing Paper: New Developments in UK Law April 2000, www.jisc.ac.uk
- Electronic Frontier Foundation, Crime and the Computer: The Unauthorised Access Offence, <http://www.strath.ac.uk/Departments/Law/dept/diglib/book/criminal/crim15.html>
- Senior Management Briefing Paper 14: The Regulation of Investigatory Powers (RIP) Act 2000: Email and Telephone Monitoring, JISC Published 2 Jul 2001
http://www.jisc.ac.uk/index.cfm?name=pub_smbp_ripa
- Law-bytes, Computer Misuse and Extradition, Wrigley Claydon - Solicitors Oldham and Todmorden, <http://www.swarb.co.uk/lawb/cpucmaExtradition.shtml>

- Asian School of Cyberlaws, Cyber Crime Cases, Emerging Jurisprudence, http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm

III. SECURITY OF INFORMATION INFRASTRUCTURE

DATA SECURITY, PRIVACY & CONFIDENTIALITY

International

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981
- Convention on Cybercrime 2001
- [UN Guidelines concerning computerized personal data files](#)

EU

- [Directive 95/46/EC](#) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
- Directive 2002/20 of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)
- Directive 2002/19 of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)
- 27/08/2002, Proposal for a Council Framework Decision on attacks against information systems
- European Convention on Human Rights
- Rechnungshof C-465/00, 20 May 2003

UK

- Data Protection Act 1998
- Privacy and Electronic Communications (EC Directive) Regulations 2003

- Durant v Financial Services Authority 2003 EWCA Civ 1746
- Academy Credit Limited, Chichester Crown Court on 18 December 2001

US

- The Fourth Amendment of the US Constitution effectively protects the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures [...].
- [Electronic Communications Privacy Act 1986, 18 U.S.C. Secs. 2510-2711 \(1988\)](#) (ECPA)
- Steve Jackson Games, Inc. v. United States Secret Service 816 F. Supp. 432 (W.D.Tex. 1993), aff'd, 36 F.3d 457(5th Cir. 1994)
- Davis v Gracey 111 F.3d 1472 (10th Cir. 1997)
- McVeigh v. Cohen No. 98-116 (D.D.C. Jan. 26, 1998)

Romania

- Law 504/2004 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector
- Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data

France

- Commission Nationale de L'Informatique et des Libertés v Rampell Software

Germany

- North Rhine Westphalia Data Protection Authority v General Electric's

Secondary Sources

- Privacy International, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, 10th October 2003, Prepared by Covington & Burling, http://www.privacyinternational.org/issues/terrorism/rpt/data_retention_memo.pdf
- Privacy – The Voice of Business, Jonathan Armstrong, “Personal Data Protection – Policy and Practice in EU Accession and New Member States”, <http://privacy.gateway.bg/htmls/en/home.htm>
- Oscura News: Directors found guilty under DPA 1998 21 December 2001 http://www.oscura.co.uk/show_news.asp?news_id=9
- French Data Protection Authorities rule US email spy software unlawful Posted: 18 august 2004 <http://privacydataprotection.co.uk/news/#foreign>

- German Data Protection Authority allows foreign transfer of General Electric's employee data Posted: 29th December 2003 <http://privacydataprotection.co.uk/news/>
- Foreign Policies: e-Communications, Interconnection and Interoperability, Europe's Information Society Thematic Portal, European Commission, http://europa.eu.int/information_society/policy/ecom/todays_framework/interconnection_interoperability/index_en.htm
- Denial-of-Service Attacks Rip the Internet by Lee Garber in Technology News, Computer Magazine
- Internet Architecture WG: DoS-resistant Internet Subgroup Report by Mark Handley, University College London Cyberthreat - An investigation into the methods, perpetrators, future & prevention of cyberspace computer crime: A Bsc Final year dissertation by James John Richardson
- Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks by Cisco Denial of Service prosecution in the UK, January 19, 2005 at Out-Law.com

IV. CYBERCRIME

International

- UN Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on Combating the Criminal Misuse of Information Technology
- UN Resolutions 57/239 and 58/199 of 23 December 2003 on the Creation of a Global Culture of Security and the Protection of Criminal Information Infrastructure
- Eleventh UN Congress on Crime and Prevention and Criminal Justice, April 2005 Workshop 6: Measures to combat computer-related crime
- UN recommendations on fighting cybercrime as published by the Computer Crime Research Center in May 2005
- Council of Europe Convention on Cybercrime 2001

EU

- Article 29 of the Treaty on the European Union
- Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions was issued for creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime 26/01/2001
- Communication from the Commission Preventing fraud and counterfeiting of non-cash means of payment 9.2.2001

- Proposal for a Council Framework Decision on the European arrest warrant and the surrender procedures 19.9.2001

US

- Wire Fraud¹ 18 U.S.C. 1343
- Mail Fraud 18 U.S.C. 1030
- Financial Institution Fraud 18 U.S.C. 1341
- Access Device Fraud 18 U.S.C. 1344
- Computer Fraud and Abuse 18 U.S.C. 1029
- Identity Theft²⁷⁸
- Aggravated Identity Theft²⁷⁹ Act
- United States v. Forcellina²⁸⁰
- United States v. Hill²⁸¹
- United States v. Carr²⁸²
- United States v. Guevara²⁸³
- United States v. Gebrezihir²⁸⁴
- United States v. Kalin²⁸⁵
- United States v. Butcher²⁸⁶
- United States v. Christensen²⁸⁷
- Federal Trade Commission v Audiotech Connection Inc²⁸⁸
- R. v Governor of Brixton Prison, Ex parte Levin²⁸⁹

UK

- Computer Misuse Act 1990

China

- Criminal Code Article 286

Japan

- Japanese Penal Code February 2000²⁹⁰
- Anti-Hacking Law 2003

²⁷⁸ 18 U.S.C. 1028(a)(7)

²⁷⁹ 18 U.S.C. 1028A

²⁸⁰ D. Conn., sentenced Apr. 30 and June 18, 2004

²⁸¹ SD Tex., sentenced May 2004

²⁸² ED Va. 2003

²⁸³ WD Wash. 2003

²⁸⁴ SDNY 2003

²⁸⁵ DNJ, Nov. 2003

²⁸⁶ 53 MJ 711, 712, 714 (AF Ct. Crim. App. 2000)

²⁸⁷ 403 F.3d 1006 (8th Cir. 2005)

²⁸⁸ *E.D.N.Y. Filed 13 February 1997*

²⁸⁹ [1996] 3 WLR 657

²⁹⁰ Privacy International, Country Reports, Japan, <http://www.privacyinternational.org/survey/phr2000/countrieshp.html>

Australia

- Australian Securities and Investments Commission v Steven George Hourmouzis.
- Securities and Exchange Commission v World Financial & Investment Co., Inc. and Victor M. Wilson US District Court, EDNY, No. 99 CIV 7608 (ILG)

Secondary Sources

- Loose Wire, Dogbert Goes Phishing, Jeremy Wagstaff, August 12, 2005, <http://loosewire.typepad.com/blog/phishing/>
- BBC News, Phishing Pair Jailed for ID Fraud, 29 June 2005, http://news.bbc.co.uk/2/hi/uk_news/4628213.stm
- Anti-Phishing Working Group, What is Phishing & Pharming?, <http://antiphishing.org/>
- Phishing: A Growing Threat to Financial Institutions and E-Commerce by Frederick W. Stakelbeck, Jr., Training and Development Coordinator, December 2004, <http://www.phil.frb.org/src/srcinsights/srcinsights/Phishing%20-%20Dec%2004.pdf>
- Cybercrime law: A Global Survey of Cybercrime legislation, Chief Judge Stein Schjolberg, <http://www.cybercrimelaw.net/index.html>
- Moss tingrett, Moss District Court, The Legal Framework – Unauthorised Access to Computer Systems, Penal Legislation in 44 countries, Judge Stein Schjolberg, April 7, 2003
- Asian School of Cyberlaws, Cybercrime Cases: Emerging Jurisprudence, http://www.asianlaws.org/cyberlaw/library/cc/cc_caselaw.htm
- Computer Misuse and the Criminal Law, <http://www.cosgrave.com/courses/ProfIssues/Computermisuseandthecriminallaw.html>
- Internet Laws, Laws and Case Law, Bogdan Manolea, <http://www.legi-internet.ro/en/laws.htm>
- Privacy and Human Rights 2004: Romania, Bogdan Manolea with assistance from Cedric Laurant http://www.legi-internet.ro/privacy_ro2004.htm
- Europa, Fight Against Cybercrime, <http://europa.eu.int/scadplus/leg/en/lvb/l33193b.htm>
- Europa, Cybercrime European Commission, Anti cybercrime legislative proposals on Council table, http://europa.eu.int/comm/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm
- EurActiv, Finance Fraud, 9 June 2005, <http://www.euractiv.com/Article?tcaturi=tcu:29-140752-16&type=LinksDossier>
- Legaldays, E-Commerce Regulations - E-Comm Regulations - Electronic Commerce Directive - Policy – Legislation, <http://www.legaldays.co.uk/current/e-commerce.htm>

- The Institute of Internal Auditors UK and Ireland Online, Auditors blow whistle on fraud, 19 May 2003,
http://www.iaa.org.uk/about/presscentre/recentarticles.cfm?Action=1&ARTICLE_ID=1164
- Peterborough UK, European Court to review anti-fraud legislation, August 2004,
<http://www.peterborough.net/business/articles/antifraud.asp>
- Avoid Identity Theft, Identity Theft Legislation, <http://www.avoid-identity-theft-guide.com/identitytheftlegislation>
- Cybersecurities Law Tribune, Periodic News Briefs Regarding Securities Regulation and the Internet, Volume 1, Issue 10 - December 11, 1999,
http://www.cybersecuritieslaw.com/oldsite/csltribune_12_11_99.htm
- US Securities and Exchange Commission, Litigation Release No. 17054 / June 26, 2001,
SECURITIES AND EXCHANGE COMMISSION V. WORLD FINANCIAL & INVESTMENT CO., INC. AND VICTOR M. WILSON, U.S. District Court, E.D.N.Y., No. 99 CIV 7608 (ILG)
- FBI, Testimony of Steven M. Martinez, Deputy Assistant Director, Federal Bureau of Investigation, Before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census September 22, 2004, <http://www.fbi.gov/congress/congress04/martinez092204.htm>
- UCLA Journal of Law and Technology, The Emerging Consensus on Criminal Conduct in Cyberspace, by Marc D. Goodman and Susan W. Brenner,
http://lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php

NB *All websites accessed between June 1, 2005 and September 14, 2005.*