# Forensics in Cyber-Space – The Legal Challenges

**INVITED PAPER**

Nigel Wilson
Barrister

Bar Chambers
34 Carrington Street
Adelaide South Australia 5000
Australia
nigel.wilson@barchambers.com.au

## ABSTRACT

The nature and impact of Information and Communication Technologies (ICTs) involve major challenges and opportunities for forensic analysis and legal regulation. The legal challenges for forensic analysis in cyber-space include:

- global liability issues;
- jurisdiction–based issues;
- risk issues;
- data and document retention issues;
- response and regulatory issues;
- independence, objectivity and expertise issues;
- commercialization issues;
- regulatory and investigation issues; and
- human rights issues.

The opportunity exists for forensic analysis to play a key role in the regulation of cyber-space and the management of cyber-risk.

## 1. CYBER-SPACE AND THE INFORMATION AGE

In order to identify the legal challenges which may arise in the future in the field of forensic analysis in cyber-space it is important to seek to understand the current legal framework, modern society and the workplace environment, both internationally and locally.


E-FORENSICS 2008, January 21-23, Adelaide, Australia

DOI 10.4108/e-forensics.2008.2926

A vast amount of work has been done and time and resources have been invested by international agencies and national governments in examining the likely impact of Information and Communication Technologies (ICTs) on the workplace of the future and on the human condition.[1]

A key feature of the stated international position regarding the regulation of cyber-space and ICTs is the need for the protection of human rights, particularly the right to privacy.

### 1.1 Regulating Cyber-space - The International Position

Historically, periods of major international conflict have been marked by ICT development and growth either at the time or shortly thereafter. In the post-World War II period, it was resolved by Article 12 of the Universal Declaration of Human Rights (1948) that:

> *"No-one shall be subjected to arbitrary interference with his/her privacy, family, home or correspondence, nor to attacks upon his/her honour or reputation. Everyone has the right to protection of the law against such interference or attacks."*

Article 17 of the International Covenant on Civil and Political Rights (1966) is to similar effect.

In 1997 then United States President Bill Clinton stated a framework for global economic commerce and identified five core principles:

- the private sector should lead;
- governments should avoid undue restrictions on electronic commerce;
- where government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce;
- governments should recognize the unique qualities of the internet;
- electronic commerce over the internet should be facilitated on a global basis.[2]

More recently, the United Nations General Assembly resolved in the Millennium Declaration in 2000:

> *"To ensure that the benefits of new technology, in conformity with the recommendations contained in the Economic and Social Council (ECOSOC) 2000 Ministerial Declaration, are available to all."*

The ECOSOC 2000 Ministerial Declaration stated that ICTs:

- are central to the emerging global knowledge-based economy;
- can accelerate growth;
- can promote sustainable development;
- assist in eradicating poverty in developing countries and countries in transition.

However, the following key issues and concerns were identified:

- the *"new economy"* creates opportunities for economic growth and social development;
- the majority of the world population still lives in poverty and remains untouched by the ICT revolution;
- there was a potential for economic development by developing countries to close the *"digital divide"* and in so doing ICTs should be utilized to foster *"digital opportunity"*.

Subsequently, the United Nations General Assembly resolved that legal systems should:

- protect the confidentiality, integrity and the availability of data and computer systems from unauthorized impairment;
- ensure that criminal abuse is penalized.[3]

Forensic analysis will play a critical role in all components of modern society, the economy, the workplace and the home environment and their regulation from the development and protection of ICTs, investigation and detection of unauthorized or unlawful activity and, ultimately, prosecution and litigation.

## 1.2 Regulating Cyber-space - The Australian Position

The common law and general Australian legislation has been readily applied to the modern cyber-space environment. Where necessary, specific legislation has been enacted which prohibits practices which are not in the public interest. Some of this legislation reflects general human rights principles and, in effect, prohibits behaviour or conduct which constitutes inappropriate and unwelcome interferences with an individual's privacy, family, home or correspondence. For example, specific legislation has been enacted to prohibit:

- "spam" - making it illegal to send or cause to be sent *"unsolicited commercial electronic messages";* [4] and
- unsolicited telemarketing calls - making it illegal to make unsolicited telemarketing calls to numbers listed on the register.[5]

# 2. CYBER-SPACE IN PERSPECTIVE

The pace of technological change and its influence on the modern society can be demonstrated by analyzing, specifically, the short history but immediate impact of telephones, computers and the internet in modern society. An appreciation of the impact of the ICT revolution to date can assist in planning for and coping with future developments. The identifiable trends to date include: constant innovation, speed of growth and change, scale of activity and production, high risk but possible high return, global impact and the benefit of predictable, uniform regulatory frameworks.

## 2.1. Telephone

The telephone was invented in 1876 by Alexander Graham Bell. By 1880 the Bell Company had leased 100,000 instruments.

By contrast, in 2007 Apple's new *"Iphone"* is estimated to have sold between 500,000 to 700,000 units in the first weekend of its sales. Each phone retailed for approximately US$499 to US$599. Accordingly, approximately US$250 million in sales are estimated to have occurred in one weekend alone.

Trends in the relative cost of telephone usage also demonstrate the vast economies of scale in the international telecommunications system. The cost of a telephone call from New York to London was approximately a dollar in 1950, six cents in 1990 and is essentially "free" today using the internet.

## 2.2. Computers

The first rotor machines were the subject of the Enigma patent in 1918.

During World War II electro-mechanical *"bombes"* were developed together with the top secret Colossus computer. The Electronic Numerical Integrator and Computer was developed between 1943 and 1946.

By 1965 Intel founder, Mr Graham Moore, described what became known subsequently as *"Moore's law"*: that the number of transistors on a computer chip doubles every two years. As a result, a musical birthday card bought today has more computing power than the fastest main frame computers of the 1970s.

## 2.3. The Internet

The internet was invented in 1969 and used predominantly for email and file transfers. The HTTP (Hypertext Transfer Protocol) and HTML (Hypertext Markup Language) protocols were developed in 1989. Business to consumer (B2C) and business to business (B2B) data exchange, communication and commerce has spawned as a result.

In March 2000 the *"dot.com bubble"* burst. However, the rate of internet usage is burgeoning. The 2006 Australian census determined that 58% of Australian households had an internet connection.[6] In 2007 it is reported that nearly a billion people use digital technology in their daily lives. Further, despite *"the notorious dotcom collapses, estimates show that worldwide online trade exceeded US $2000 billion in 2002 with predicted increases*

*in excess of US $12,800 billion by 2006: the European Union alone is expected to experience on-line trade rising from €77billion in 2001 to €2.2trillion by 2006"*.[7]

# 3. OTHER TRENDS IN THE CYBER-WORKPLACE AND SOCIETY

The technology changes occurring in the cyber-workplace and society are also occurring at the same time as a number of other significant changes.

Major studies have identified the following trends:

- a shifting workforce composition including an older workforce and an ageing population together with an increasingly female participation in the workforce;
- an increasingly skilled workforce with emphasis on "*knowledge*" based industries;
- organisational changes in which firms are becoming more specialized and are increasingly vertically disintegrated;
- the nature of the employment environment has changed from the traditional employer-employee relationship towards an increasing use of independent contractors, temporary workforce and, in some industries, "*e-lancing*";
- work locations now include temporary locations and "*remote*" workplaces;
- workplace education and training now includes ICT-based training.[8]

These trends must also be borne in mind in seeking to identify the legal challenges facing forensic analysis in cyber-space.

# 4. LEGAL CHALLENGES FOR FORENSIC ANALYSIS IN CYBER-SPACE

The legal challenges for forensic analysis in cyber-space include:

- global liability issues;
- jurisdiction – based issues;
- risk issues;
- data and document retention issues;
- response and regulatory issues;
- independence, objectivity and expertise issues;
- commercialization issues;
- regulatory and investigation issues; and
- human rights issues.

## 4.1. Global Liability Issues

Globalisation of commerce and trade gives rise to a potential liability in every jurisdiction in which a website is viewed or an email is published.[9] Provided the jurisdictional basis exists, existing consumer protection legislation has the capacity to apply extra-territorially. For example, to misleading advertising on the internet[10] and to the operation of websites outside a country's jurisdiction engaging in inappropriate business practices.[11] Courts have recognized the need for international co-operation in meeting the needs of consumers in the internet world[12] and have applied and enforced laws against companies and individuals located within a jurisdiction but operating outside that jurisdiction.[13]

Forensic experts have the capacity and capability to be involved in global analysis and work in international environments. For this to be achieved effectively, co-operation and comity will be required between countries and their national regulatory and investigative agencies and organizations.

## 4.2. Jurisdiction – based issues

The cyber-space environment raises issues regarding the location of data and information. For example, the location of the "*worker*" may differ from the location of his or her employer. Further, "*home*" offices and ICTs located within them may contain important data and information which may be owned by the employer or others. Further, insurance policies which may apply to e-risk events arising from cyber-space activities are usually jurisdiction-specific and contain United States exclusions. The internet is often described as "*borderless*".

## 4.3. Risk Issues

Risk issues for cyber-space include viruses damaging own systems and being forwarded to third parties. Third parties (hackers etc) have the capacity to damage systems through unauthorized access, sabotage and identity theft. Data protection of confidential information will be paramount. The detection of fraud and other criminal practices will be a key consideration.[14]

The protection of intellectual property is the subject of considerable international regulation and comity but the relative ease with which ICTs can be reproduced or reverse-engineered and their relatively short operational life mean that enforcement is often not effective or timely.[15]

If an "e-risk" event occurs within an organisation the possible financial consequences include trading losses, business interruption, personnel downtime, data retrieval costs, reputation loss and restoration or remedial costs. The organisation the subject of such an event may itself be responsible to other parties (eg customers or clients for privacy intrusions or suppliers to whom duties of care or contractual obligations are owed).

## 4.4. Data and Document Retention Issues

The *"paperless office"* has become an expression which has not been reflected in reality. Innovation in rights management of documentation and the ability of software to control the recipient of a document and how long it is accessible[16] gives rise to issues regarding data and document retention. In subsequent litigation, failure to establish suitable policy and system control procedures including control of access to relevant databases, programs, logging of changes, backup practices and audit procedures can give rise to documents being rendered inadmissible.[17]

## 4.5. Response and regulatory issues

The need for a speedy and often immediate response to protect and retrieve data and ICTs themselves is heightened in the cyber-space environment. In many situations, *ex parte* procedures (i.e. without notice to the opposing party) to protect or retrieve property or data are required. Records of steps taken in response to cyber-risk events should be documented, auditable, preserved and protected. Evidence will often need to be given by those engaged to investigate and conduct forensic analysis of the steps they have taken and the adequacy and integrity of those procedures.

Compliance with all regulatory provisions will be necessary to ensure that the information obtained can be used effectively and lawfully. For example, in the area of criminal investigations and prosecutions, compliance with procedural requirements relating to criminal investigations (search warrants and proper cautions to an accused etc) must be complied with at all times. In the civil and commercial law area, compliance with regulatory provisions is also necessary and often will involve considerations of commercial sensitivity of data and privacy concerns.

## 4.6. Independence, objectivity and expertise issues

Forensic investigations and analysis which are not conducted in accordance with verifiable and established practices and principles are likely to be challenged and could be ruled inadmissible or be held to amount to an abuse of process in extreme situations. Whilst the judicial process is by its nature an "adversarial" one and involves the parties to the litigation "taking sides", it is vital that forensic experts and analysts conduct themselves ethically, independently, impartially and professionally. The guidelines for experts which have been promulgated by all courts in Australia requiring objectivity, independence and impartiality should be followed at all times.

## 4.7. Commercialisation issues

Whilst forensic analysis of cyber-space issues has an immediate benefit in dealing with the task under consideration, often there are broader applications which have greater value and possible return. The ownership of forensic techniques and methods and their protection, whether by intellectual property laws or confidentiality provisions and employment regimes, raise important questions which are complex and often raise ethical considerations. For example, effective "data-mining" of vast quantities of data and information has immense value to businesses and governments in all areas of human activity ranging from areas as diverse as product promotion and marketing to criminal profiling and health research.

## 4.8. Human rights issues

Until recently, domestic regulation of the workplace has not emphasized individual human rights. The common law has been reluctant to protect an individual's right to privacy.[18] However, an increasing number of jurisdictions are adopting international principles of human rights into domestic law.

Common law protection of an individual's right to privacy has been inconsistent. General legislation protecting privacy has the capacity to regulate breaches of privacy principles.[19] The central concept in the protection of privacy is the notion of personal information which is information or an opinion which identifies an individual or allows their identity to be readily worked out from the information. In the event of failure to comply with the principles then the Privacy Commissioner has the power to investigate a complaint or investigate on the Commissioner's own initiative an act or practice that may be a breach of privacy (even if no complaint is made) and seek an order (injunction) from the court to stop conduct that does or would breach the Privacy Act. For example, inadvertent disclosure of customer email addresses has been sanctioned.[20]

In addition, some jurisdictions have recently enacted human rights legislation which is reflective of the international charter of human rights in which the right of a person not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with is protected.[21]

The adoption of broad human rights principles raises complications for the regulation of ICTs:

- some jurisdictions have ratified international human rights conventions but have not legislated for their application domestically;[22]
- the expense and delay involved in the enforcement of human rights principles;
- the perception that human rights principles involve public law concepts (eg. judicial review) rather than private law rights and remedies including rights to compensation;
- the interpretation and enforcement of human rights principles has been far from predictable, simple and consistent.

The "open-textured" nature of human rights principles raises particular challenges in a regulatory and forensic environment where speed of application and certainty of decision-making are of critical importance.

# 5. THE ROLE OF FORENSICS IN RISK MANAGEMENT

Forensics also has a role in anticipating cyber-risk and managing e-risk events prior to litigation being considered or commenced.

As with all risk management, the key elements for risk management of cyber-space events will include:

- appropriate training and supervision;
- assessment of the threat, system characteristics and the physical and cyber environments in which those systems operate in a documented and comprehensive manner;[23]

- effective protocols and compliance. Specifically, in relation to ICTs these include:
    - closed networks;
    - intranets;
    - firewalls;
    - anti-virus protection;
    - digital signatures; and
    - encryption security
- maintenance procedures and systems including for managing and dealing with security breaches.

The inter-relationship in modern society between critical infrastructures (electric power, gas supply, water supply and waste treatment, rail transport and ICTs) has been described as "*mutually and circularly dependent*". The International Risk Governance Council has concluded that "*… our societies are most vulnerable to disruptions of electric power supply and disruptions to, or degradation of, ICT services*". It was their judgment that "*a significant problem for owners, managers and regulators is that the public and many officials in government have limited knowledge of the vulnerabilities of these systems and of the risk factors that have increased during the past several decades.*"[24] The challenge for individuals, businesses and governments will be to identify relevant risks and to put in place appropriate risk management strategies or policy frameworks. Governments, businesses and organizations which are forensically astute will be better able to identify and deal with these challenges.

## 6. CONCLUSION

Cyber-space has the very real prospect of leading to a digital divide rather than fostering digital opportunity. The identification and regulation of legal issues will present a key challenge to the equitable allocation of ICTs worldwide. A fundamental factor in the success of such a worthwhile goal is an awareness of the relevance, and consistent application, of human rights principles to an area which has historically been marked by a "*survival of the fittest*" and a "*first to market*" mentality.

What cannot be overlooked is that human rights "*should be seen as informing almost everything lawyers and courts do*".[25] Forensic specialists and experts will also need to appreciate these issues and be mindful of them in their analysis.

One individual whose corporation has so revolutionized the workplace and been a driving and dominant force in the ICT phenomenon has said:

> "*During the last decade, digital technology has changed the world in profound and exciting ways. Today we communicate instantly with people we care about without worrying about the traditional limitations of time and location. At work, we collaborate with colleagues in distant cities ... But these changes are just the beginning.*"[26]

If the current stage of ICT development is in its infancy, then the challenge to society and the legal environment of forensic investigation and analysis, regulation and risk management will be to strike a balance between encouraging innovation and competition and upholding legal rights in cyber-space, particularly the protection of fundamental human rights.

## 7. NOTES

This paper is a revised and updated version of a paper presented by the author in December 2007 at the Second International Conference on Legal, Security and Privacy Issues in Information Technology held in Beijing, China. The paper was entitled "The Workplace of the Future – Liability Issues and Risk Management" and has recently been published in "Cyberlaw, Security and Privacy" (Edited by S. Kierkegaard), 2007.


[1] United Nations, Information Economy Report 2005 Chapter 5; Rand Corporation (2004), The 21st Century at Work: Forces Shaping the Future Workforce and Workplace in the United States; Irish National Centre for Partnership and Performance (2005) Working to our Advantage – A National Workplace Strategy: Report of the Forum of the Workplace of the Future.

[2] See http://www.technology.gov/digeconomy/framewrk.htm

[3] United Nations General Assembly Resolutions 55/63 (2001) and 56/121 (2002)

[4] See the *Spam Act 2003* (Commonwealth of Australia).

[5] See the *Do Not Call Register Act 2006* (Commonwealth of Australia).

[6] Australian Bureau of Statistics, (2007) Media Release 070628CA-8093

[7] Smith, Regulating E-Commerce in the WTO: Exploring the Classification Issue in Graham and Smith, (2004) Competition, Regulation and the New Economy, Hart Publishing at 159.

[8] Rand Corporation (above, note 1).

[9] See observations made by the High Court of Australia in *Dow Jones & Company Inc v Gutnick* (2002) 210 CLR 575.

[10] *Australian Competition and Consumer Commission v Hughes* [2002] FCA 270.

[11] *Australian Competition and Consumer Commission v Chen* [2002] FCA 1248.

[12] *Australian Competition and Consumer Commission v Chen* (above, note 10).

[13] *World Play Services Pty Ltd v Australian Competition and Consumer Commission* [2005] FCAFC 70.

[14] For example, an employer was found vicariously liable for the fraud of its employee who accessed and transferred monies from the bank account of a person for whom she was responsible for caring: *Ffrench v Sestilli* [2007] SASC 241.

[15] Views are divided amongst industry experts about the effectiveness of regulation and protection of intellectual property in the face of escalating internet piracy: see J Torr, (2005) Internet Piracy, Thomson Gale.

[16] B. Gates, Chairman, Microsoft Corporation, Enabling Secure Anywhere Access in a Connected World (6 February 2007): See http://www.microsoft.com/mscorp/execmail/ 2007/02-06secureaccess.mspx.

[17] *American Express v Vinhnee* 336 BR 437 16 December 2006 9th Circuit.

[18] A common law right to privacy was left open by the High Court of Australia in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. Subsequent cases in the State Supreme Courts of Australia have in one instance upheld a right to privacy (*Grosse v Purvis* [2003] QDC 151) and in another case in a different State of Australia not found a right to privacy (*Giller v Procopets* [2004] VSC 113).

[19] See the *Privacy Act 1988* (Commonwealth of Australia).

[20] *O v Large Retail Organisations* [2004] Priv Cmr A 2.

[21] *Charter of Human Rights and Responsibilities Act 2006* (Victoria); *Human Rights Act 2004* (Australian Capital Territory)

[22] Eg Australia. See Hettiarachi, "Some Things Borrowed, Some Things New: An Overview of Judicial Review of Legislation under the Charter of Human Rights and Responsibilities (2007) OUCLJ 61 at 66.

[23] Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Special Publication 800-30, January 2002 and more recently International Organization for Standardisation and International Electrotechnical Commission ISO/ IEC 27002:2005 (July 2007)

[24] International Risk Governance Council (2006), Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures (White Paper No.3).

[25] M Warren AC, "Introduction to Human Rights Law: Seminar – Part 1" (2007) 81 ALJ 245 at 246.

[26] B Gates, Chairman, Microsoft Corporation 6 February 2007, see note [16] above.