The Cyber-Workplace – Identifying Liability Issues in the Information Age and Managing E-Risk

Nigel Wilson
Barrister, Bar Chambers, Australia, nigel.wilson@barchambers.com.au

Follow this and additional works at: https://commons.erau.edu/adfsl

Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

Scholarly Commons Citation
https://commons.erau.edu/adfsl/2008/friday/3

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu, wolfe309@erau.edu.
The Cyber-Workplace – Identifying Liability Issues in the Information Age and Managing E-Risk

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

ABSTRACT
The information age provides numerous opportunities for modern society but also presents significant challenges in identifying liability issues and in managing risk. Technological change has occurred rapidly and is continuing at the same time as other major trends and changes are taking place in society and, in particular, in the workplace. The prospect of global liability and the complexity of jurisdictional differences present a considerable hurdle to the uniform regulation of liability issues. General legislation and legal principles have been readily applied to the cyber-world and to modern business practices and the workplace. Where necessary, legislatures have introduced specific legislation to regulate unfair or inappropriate business and workplace practices which involve the use of technology in an unsuitable manner. Consistent with international objectives, a central element of the regulation of e-commerce and the cyber-space economy will be the protection of individual human rights, particularly the right to privacy. Human rights concepts raise special challenges in relation to the regulation of the modern, technology-intensive economy and workplace. Appropriate data protection and document retention policies will be a critical component of effective risk management and compliance programs in the information age.

1. THE CYBER-WORKPLACE
A vast amount of work has been done and time and resources have been spent by International agencies and national governments in examining the likely impact of Information and Communication Technologies (ICTs) on the modern workplace and the human condition.[1] A key feature of the stated international position regarding the regulation of cyber-space and ICTs is the necessity for the protection of fundamental human rights, particularly the right to privacy.

1.1 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 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 electronic commerce in which five core principles were identified:

- 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 information and communication technology (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]

1.2 Regulating the Cyber-Workplace at the National Level

In both common law and civil law jurisdictions around the world existing general laws have been readily applied to the modern economy and the cyber-space environment. When necessary, specific legislation has been enacted to prohibit or regulate practices which are not in the public interest. Some of this legislation reflects general human rights principles and, in effect, prohibits or regulates behaviour or conduct which constitutes an inappropriate or unwelcome interference with an individual’s privacy, family, home or correspondence.

2. THE IMPACT OF TECHNOLOGY ON MODERN SOCIETY IN PERSPECTIVE

The pace of technological change and its increasingly ready acceptance can be demonstrated by analyzing, specifically, the short history but immediate impact of telephones, computers and the
internet on 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, increasing (often exponential) 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 only 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 “bombe” 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. In 2006 58% of Australian households had an internet connection.[4] 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.”[5]

3. OTHER MAJOR TRENDS IN THE MODERN WORKPLACE

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 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.[6]

These trends must also be borne in mind in seeking to understand the way in which modern business is conducted and to regulate its activities.

4. LIABILITY ISSUES IN THE MODERN WORKPLACE

Until recently, domestic regulation of modern business activities has not emphasized individual human rights. The common law has been reluctant to protect an individual’s right to privacy.[7] However, an increasing number of jurisdictions are adopting international principles of human rights into domestic law.

The liability and regulatory issues for the information age include:

- global liability issues;
- jurisdiction – based issues;
- risk issues;
- data and document retention issues;
- 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.[8] Provided the jurisdictional basis exists, current consumer protection legislation has the capacity to apply extra-territorially, for example, to misleading advertising on the internet[9] and to the operation of websites outside a country’s jurisdiction engaging in inappropriate business practices.[10] Courts have recognized the need for international co-operation in meeting the needs of consumers in the internet world[11] as well as the need to regulate companies located within a jurisdiction but operating outside that jurisdiction.[12]

4.2 Jurisdiction – based issues

Modern commerce is being conducted on an international basis. The cyber-space environment raises issues regarding the location of the “worker” and the data or transactions in which they are involved. Each of these may differ from the location of the employer. Further, “home” offices and ICTs may contain important information which may be owned by the employer or others. The “home” office may not satisfy specific occupational health and safety regulations which may apply in the employer’s office or traditional workplace. Further, insurance policies which may apply to e-risk events arising from economic activity are usually jurisdiction-specific and contain United States exclusions. The internet is often described as “borderless”.

4.3 Risk Issues

Risk issues for the modern economy include viruses damaging own systems and being forwarded to third parties. Third parties (hackers etc) have the capacity to damage systems through unauthorized access and sabotage. Data protection of confidential information will be paramount. The detection of fraud and other criminal practices will be a key consideration.[13] The protection of intellectual property is the subject of considerable international regulation and comity but the relative ease with
which technological innovation can be reproduced or reverse-engineered and the relatively short operational life of new technologies mean that enforcement is often not effective or timely.[14]

If an “e-risk” event occurs within an organization the possible financial consequences include trading losses, business interruption, personnel downtime, data retrieval costs, reputation loss and restoration or remedial costs. The organization 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 data and documentation and the ability of software to control the recipient of a document and how long it is accessible[15] gives rise to issues regarding data and document retention. In subsequent litigation, the 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.[16]

4.5 Human rights issues

Common law protection of a right to privacy has been inconsistent.

General legislation protecting privacy has the capacity to regulate breaches of privacy principles.[17] 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, for example in Australia, the Privacy Commissioner has the power to investigate a complaint or investigate on the Commissioner’s own initiative an act or practice which 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 principles. For example, inadvertent disclosure of customer email addresses has been sanctioned.[18]

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.[19] For example, specific legislation has been enacted to prohibit:

- “spam” making it illegal to send or cause to be sent “unsolicited commercial electronic messages”; [20]
- unsolicited telemarketing calls making it illegal to make unsolicited telemarketing calls to numbers listed on the register.[21]

The adoption of broad human rights principles raises complications for regulation in the information age:

- 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.
5. RISK MANAGEMENT

As with all risk management, the key elements for risk management of liability issues in the cyber-workplace 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 modern technology 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.

6. CONCLUSION

Cyber-space has the very real prospect of leading to a digital divide between nations and the people within them rather than fostering digital opportunity. The identification and regulation of liability issues will be a key component of the equitable allocation of ICTs worldwide. A fundamental factor in the successful achievement of such a worthwhile goal will be 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] This includes the regulation of the modern business and work-place environment both now and in the future.

One individual whose corporation has so revolutionized the modern economy and has been a driving and dominant force in the information age 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.”[24]
If the current stage of ICT development is in its infancy then the challenge to society and the legal environment of regulation, liability allocation and risk management will be to strike a balance between innovation and competition and the protection of fundamental human rights in the modern economy and the cyber work-place.

NOTES

This paper is a revised and updated version of two papers presented by the author in December 2007 and January 2008.

The first paper was presented in December 2007 at the Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) which was held in Beijing, China. The LSPI paper was entitled “The Workplace of the Future – Liability Issues and Risk Management” and was published in the conference proceedings book “Cyberlaw, Security and Privacy” (Edited by S. Kierkegaard), 2007. The LSPI paper is to be published in 2008 in the International Journal of Liability and Scientific Enquiry.

The second paper was presented in January 2008 at the E-Forensics 2008 Conference (The First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia) at the University of Adelaide in Adelaide, South Australia.

REFERENCES

[7] 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).
[13] 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.