The Council of Europe Draft Convention on Cyber-Crime: A European perspective on a global problem

Jane Rawlings

Jane Rawlings is a solicitor specialising in Information Technology and E-commerce.

1. Introduction

> *"These developments [in information technology] have given rise to unprecedented economic and social changes but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries. The recent spread of detrimental computer viruses all over the world has provided proof of this reality. Technical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour."*

Paragraph 5 of the Draft Explanatory Memorandum of the European Committee on Crime Problems to the 27th and final version of the Council of Europe's Draft Convention on Cyber-Crime[1].

> *"These cyber-space offences are either committed against the integrity, availability, and confidentiality of computer systems and telecommunications networks or they consist of the use of such networks or their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."*

From Decision CDPC/103/211196 of the European Committee on Crime Problems of the Council of Europe, November 1996.

Even a casual search of the newspapers and the Internet demonstrates the truth of the statements above. The global pervasiveness of cyber-crime is demonstrated by the activities of the author of the "Love Bug" and "Kournikova" viruses, the defacements of websites in the Australia, the United States and Europe by hackers such as PoizonBox and Lee Ashurst, from Oldham in the United Kingdom, who blocked web access for all citizens of the United Arab Emirates by hacking into the servers of the country's only ISP, Etisalat[2]. There are perceived problems both with the international cooperation of law enforcement agencies in the detection and prevention of cyber-crime and whether they have the training and knowledge to deal with cyber-crime. The truth of the statements above is also reflected in the lack of a truly global standard for computer crime offences and computer related criminal offences.[3]

On 26 June 2001, the European Committee on Crime Problems ("CDPC") of the Council of Europe formally adopted the 27th and final version of the Draft Convention on Cyber-Crime (the "Cyber-Crime Convention"). The Cyber-Crime Convention will now be recommended to the Council of Europe's 43 member countries for signature[4]. It may also be signed by Canada, the United States and Japan – which have observer status - and South Africa. It is likely that the Committee of Ministers of the Council of Europe will examine and probably adopt the Cyber-Crime Convention in September 2001. At that time, the Council of Europe's Committee of Ministers may also decide to open the convention for signature in Budapest at the end of November 2001.[5] The Council of Europe's Cyber-Crime Convention will enter into force when 5 states, including at least 3 Council of Europe member states, have ratified it.[6]

It is likely that the Cyber-Crime Convention may form the model for a global cyber-crime convention.[7] Certainly if adopted by the Council of Europe members and by the observer states, it will cover a substantial portion of the world's computer and telecommunications systems.

2. The Structure of the Cyber-Crime Convention

The Cyber-Crime Convention covers three main areas:

(i) the creation of a baseline criminal law standard in signatory states for "cyber-crime", by harmonisation of national criminal law relating to both computer crime and offences committed by use of computers and telecommunications systems;

(ii) new procedures and rules providing for domestic investigatory powers necessary to assist the investigation and prosecution of computer crime; and

(iii) new rules to set up a regime for international cooperation in the detection and prosecution of cyber-crime.

3. Harmonisation of National Criminal Law

Articles 2 to 11 of the Cyber-Crime Convention deal with the confidentiality, integrity and

availability of computer data and systems. Articles 2 to 6 create "computer specific" offences of:

(i) illegal access, (Article 2);
(ii) illegal interception, (Article 3);
(iii) data interference, ie damage to computer programs and data (Article 4);
(iv) system interference, ie serious hindering of the function of a computer system (Article 5); and
(v) misuse of devices, ie "hacker tools" and access data for the purpose of committing the Article 2 – 5 offences (Article 6).

Articles 7 and 8 deal with "computer related" offences where computer systems and telecommunications systems are used in the commission of the offences of forgery (Article 7) and fraud (Article 8).

Articles 9 and 10 deal with "content related" offences relating to child pornography, copyright and related rights infringement. There are no offences relating to the use of computer systems in race hatred crimes or xenophobia.

Article 11 deals with the offences of attempt and aiding or abetting the commission of offences under Articles 2-10.

Each Article requires a Party to the Cyber-Crime Convention to adopt "such legislative and other measures as may be necessary to establish as criminal offences under its domestic law" the offences in Articles 2-11, as well as the provisions relating to corporate liability (Article 12) and criminal sanctions (Article 13).

In fact, this harmonisation of cyber-crime offences is only at a general and low level of principle. This is not only due to the wide variety of common law, civil law and other jurisdictions to which it may be eventually applied. It is also because each Party to the Cyber-Crime Convention retains considerable flexibility in terms of what acts will be included in the offences, and whether or not they choose to require additional elements in national criminal laws such as dishonest intent,[8] or "serious harm"[9], before certain offences can be established.

3.1 "Intentionally"

Articles 2 to 9 require that in each case the criminal offence must be committed "intentionally" and "without right". The CDPC in its Draft Explanatory Memorandum to the Cyber-Crime Convention [10] explains that the concept of "intentionally" is left open to national interpretation. There may also be additional requirements of "intent" forming part of the offence. For example, Article 8 on computer related fraud, contains an additional requirement that the offender have the "fraudulent or dishonest intent of procuring, without right, an economic benefit" either for themself or for another.

Domestic criminal law may also contain further requirements of intent. For example, Article 7, (computer related forgery), permits a Party to the Cyber-Crime Convention to require an intent to defraud or similar dishonest intent before criminal liability attaches.

3.2 "Without Right"

Similarly, the express requirement in Articles 2 to 9 of the Cyber-Crime Convention, that the conduct must be done "without right", is left to the interpretation of national criminal law principles. The CDPC and its draft explanatory memorandum to the Cyber-Crime Convention briefly discusses examples of when an act might be done which is not "without right":

> "It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable like consent, self-defence or necessity, but where other principles of interest lead to the exclusion of criminal liability." [11]

The expression "without right" derives its meaning from the context in which it is used. Thus, depending upon the context, the Cyber-Crime Convention would leave unaffected acts done under lawful government authority (for example, to maintain public order, protect national security or investigate criminal offences). Most of the criticism reserved for the Cyber-Crime Convention has focused upon the procedural measures for the detection, investigation and prosecution of cyber-crime. However, the question of when an action is taken "without right" under national criminal law leaves open the possibility that both privacy abuses and human rights abuses may be perpetuated, not only in the investigation and prosecution of cyber-crime, but in the very definition of the "cyber-crime offences" themselves.

The CDPC at paragraph 38 of the Draft Explanatory Memorandum[12] states that "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised." This is clearly a concession to industry concerns over earlier drafts of the Cyber-Crime Convention. Thus, for example, in the offence of an illegal access under Article 2, there will be no access "without right" if the owner of the computer system or network has authorised "hacking" for the purpose of testing out security measures. Similarly security testing or system re-configuration may well cause serious hindering or interference to a computer system's performance but this will not be computer sabotage under Article 5 (System Interference) – unless this is "without right".

Criminal liability cannot attach to accessing a computer system that allows free and open access by the public. This is obviously and particularly the case for Internet based services which are available for access by the public, such as the World Wide Web. The CDPC quite correctly says that making a web site publicly available must involve consent to access by any other web user[13]. However, defining the limits of this "with right" access, may prove more difficult in practice. If a web page contains meta-tags or other

information that may be used by a search engine robot to gather information about that web site, then that access is "with right" because it is with consent, as this is the basis of a World Wide Web with pages interconnected by links. But under what circumstances may the act of linking, for example, by deep linking to a web site, be a form of access "without right"?[14] Or is "deep linking" a form of unauthorised access which should require an additional element of "dishonest intent" before it might be criminalised?

Similarly, the use of standard tools in commonly used communications protocols, such as cookies to enable the "personalisation" of a web site is not necessarily an access of an individual's computer system "without right". In other words, the potential breaches of privacy law principles involved in the use of cookies need not necessarily be criminalised. However the definition of "system interference" in Article 5 is sufficiently wide to include unsolicited commercial e-mail ("spam") which seriously hinders the functioning of computer systems because of its volume and frequency[15].

Not surprisingly, the definition of the offences in Articles 2 to 11 are heavily influenced by European legal concepts and treaties. For example, the offence of illegal interception of non-public communications in Article 4 stems from the right of privacy of correspondence set out in Article 8 of the European Convention on Human Rights. Article 4 applies that principle to all forms of electronic data transfer. Similarly the offence under Article 6 which deals with the use of devices or access data for the purpose of committing any of the offences in Article 2 to Article 5 is influenced by the European Union's Conditional Access Directive[16] and the Council of Europe's own European Convention on the legal protection of services based on, or consisting of conditional access[17].

3.3 Content related offences

Article 9 on child pornography is intended to strengthen and modernise existing criminal provisions regarding the commission of sexual offences against children. It reflects both international initiatives such as the Optional Protocol for the UN Convention on the rights of the child and the recent European Commission initiative on combating sexual exploitation of children and child pornography[18]. Significantly, the offence must be committed "without right" which, as the CDPC points out, is not intended to exclude existing legal defences or relevant principles that might relieve a person of responsibility. Thus a Party may take into account fundamental rights, such as freedom of thought, expression or speech and privacy. Each party may also decide not to criminalise in whole or in part:

(i) the act of procuring child pornography through a computer system;

(ii) possessing child pornography in a computer system or on a computer data storage medium;

(iii) those who produce or distribute images of those who only appear to be minors engaged in sexually explicit conduct or the use of pseudo images representing a minor engaged in sexually explicit conduct.[19]

Article 10 deals with offences relating to the infringement of copyright and related rights. Each Party has criminalised wilful infringements of copyright and related rights arising from the obligations of that party with respect to any of the international conventions that it has acceded to for the purposes of Article 10(1) and Article 10(2)[20]. It does not include infringement of moral rights such as those in Article 6bis of the Berne Convention and Article 5 of the WIPO Copyright Treaty. Article 10 refers to the requirement that the various infringements of copyright and related rights be committed wilfully rather than intentionally, as this reflects the terminology of Article 61 of the TRIPS Agreement. A Party can allow a limited exemption from criminal liability in limited circumstances such as copyright infringement by parallel import or infringement of rental rights. There must be other effective remedies in that Party's jurisdiction including civil and/or administrative remedies, providing that these do not derogate from Article 61 of the TRIPS Agreement which sets the minimum pre-existing requirement for criminal liability in this area.[21]

3.4 Ancillary liability

Article 11 deals with the offence of attempt, aiding or abetting of any of the offences created by Articles 2 to 10. Article 11(1) requires a Party to criminalise the intentional aiding or abetting of the commission of any of the offences under Articles 2 to 10 of the Cyber-Crime Convention. Those who aid or abet the commission of any of the events must also intend that the offence be committed. This means that a service provider cannot commit the offence under Article 11(1) unless they too have the same intention to commit the offence. This is consistent with the position taken on liability of ISPs and other telecommunications service providers under the European Union's Electronic Commerce Directive.[22] The offence of attempt under Article 11(2) excludes attempts at offences under Article 1 (unauthorised access), Article 6 (misuse of devices), Article 9 (1)(b) and (e) and Article 10 (copyright infringement). According to the CDPC, this is because the offence is either conceptually difficult to attempt[23] or due to national criminal laws which limit the types of offences for which attempt is punished. Given that so much of the other details of the definition of the offences has been left to national criminal law, it is not entirely clear why the offence of attempt has been limited in the Cyber-Crime Convention in this way.

Article 12 describes the extent of corporate liability[24] of a legal person for the criminal acts of employees, which are carried out by a person in a leading role and which are undertaken for the benefit of that legal person. This liability may be criminal, civil or administrative,

depending on national legal principles.[25] There are four pre-conditions for corporate liability under Article 12(1):

(i) the offence must be one of the Article 2 -11 criminal offences;
(ii) the offence must be committed for the benefit of the legal person;
(iii) the person committing the offence must be in a leading position within the legal person, such as a director (as judged by the tests of representation, or authority to take decisions or to exercise control which appear in Article 12 (a), (b) and (c)); and
(iv) the person must have acted on the basis of one of those powers.[26]

Article 12(2) is, however, rather more contentious. A legal person may also be liable for the criminal acts of its employees which are not committed by a "leading person", but by someone under their supervision. There are three pre-conditions:

(i) the offence must be one of the Article 2 -11 criminal offences, which has been committed by a natural person acting under the authority of the legal person (such as an employee or agent);
(ii) the offence must be committed for the benefit of the legal person; and
(iii) the commission of the offence must have been made possible by a "leading person" having failed to supervise the employee or agent.

A failure of supervision may be demonstrated by a failure to take appropriate and reasonable measures to prevent the commission of criminal acts by employees or agents who act within the scope of their authority. [27]

The CDPC states that Article 12(2) should not be interpreted as a charter for employer surveillance of employees,[28] in the name of avoiding corporate liability. In reality, Article 12(2) does do not control surveillance in the name of "supervision", as both privacy and human rights issues under the Cyber-Crime Convention have been left to the national legal principles of a Party. This is of particular concern for private sector employees in Australia, given the broad definition of "employee records" under the private sector provisions of the *Privacy Act 1988*[29] and the exemption of employee records from the *Privacy Act 1988* and the National Privacy Principles.[30] The definition of "employee record" refers to a record of personal information relating to the employment of any employee and includes, among other things, the employee's performance or conduct – including criminal conduct of the sort covered by the Cyber-Crime Convention. In this respect, independent contractors and agents who use an employer's computer system are in a better position than private sector employees, as they are not employees. Collection of personal information of employees' computer use by surveillance is covered by the *Privacy Act 1988*.

The "employee record" exemption applies to that section of the private sector to which the *Privacy Act 1988* actually applies. The other broad exemption from the law of privacy in Australia is, of course, the small business operators exemption[31] which will exempt businesses with an annual turnover of less than $3 million from compliance with the *Privacy Act 1988*.

Currently there is no State law which deals directly with the control of employer surveillance of the use of computer systems by employees. The NSW Law Reform Commission will shortly issue an Interim Report, which is expected to recommend a comprehensive regulatory approach to surveillance through a new *Surveillance Act*.[32] This legislation will need to balance the reasonable expectation and right of the individual to be free from surveillance, among other things, in the workplace while regulating legitimate use of surveillance technology. The NSW Law Reform Commission's opinion is that covert surveillance (where the target is unaware of the surveillance) should require the prior approval of a court or similar body. The overall scheme of the proposed *Surveillance Act* is said to be similar to that of the *Workplace Video Surveillance Act 1998 (NSW)*.[33] However a *Surveillance Act* of this type will apply only to NSW (although similar proposals are said to be being considered in Victoria). The other States and Territories do not currently have proposals for similar legislation.

4. Procedural Rules and International Assistance for the Detection, Investigation and Prosecution of Cyber-Crime

Chapter II of the Cyber-Crime Convention sets out procedural measures which a party must implement at the national level for the criminal investigation of cyber-crime. It extends not only to the criminal offences created by Articles 2-11, but also to other criminal offences committed by means of a computer systems and to the collection of evidence in electronic form of any criminal offence. Chapter II, Section 2 creates procedures for:

(i) expedited preservation orders for existing computer data for up to 90 days (Article 16) ;
(ii) expedited preservation and partial disclosure of traffic data[34] associated with data communications for up to 90 days (Article 17) ;
(iii) production of stored computer data (Article 18);
(iv) search and seizure of stored computer data; (Article 19);
(v) real time collection of traffic data (Article 20); and
(vi) interception of the content of communications (Article 21).

Chapter III of the Cyber-Crime Convention sets out the general principles for international cooperation for the investigation "to the maximum extent possible" (Article 23). As with Chapter II, this

extends to the cooperation in the investigation of Article 2-11 offences, to other offences committed by means of a computer system and to evidence in electronic form of any criminal offence. This includes extradition and mutual assistance in investigation, (Articles 24 and 25) and handing over information uncovered in investigations which assists another Party in the investigation of a cyber-crime offence in its jurisdiction (Article 26). A Party may specify certain conditions and safeguards to mutual assistance (Article 27).

Some of the most vocal criticism of the Cyber-Crime Convention has been directed at the procedural rules under Chapter II as well as the international assistance provisions of Chapter III.[35] Much of this criticism has centred on the treatment of human rights and privacy issues in the Cyber-Crime Convention.

The Cyber-Crime Convention creates common investigative procedures and a framework for international assistance in the investigation and prosecution of cyber-crime. However, the privacy and human rights measures that should protect the citizens of a Party against the overzealous or wrongful exercise of investigative powers have been left to "safeguards" in a Party's national law (Article 15 of the Cyber-Crime Convention). These may be more or less effective, depending on:

(i) whether or not the Party concerned has acceded to instruments such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms or the 1966 United Nations International Covenant on Civil and Political Rights, and

(ii) the extent to which these have been implemented into that Party's national law.

The Council of Europe members are obliged[36] to implement Article 8 of the European Convention of Human Rights.[37] However, the Cyber-Crime Convention may also be signed by countries that are not members of the Council of Europe and who are not subject to the same obligations as Council of Europe members. The Article 29 Working Party of the European Commission[38] commented adversely on this approach and strongly recommended that the Cyber-Crime Convention "should contain [privacy] provisions outlining the protections that must be afforded to individuals who are subject of the information, to be processed in connection with all the measures envisaged in the Draft Convention." [39] This suggestion has not be taken up in the 27th and final draft of the Cyber-Crime Convention.

The CDPC has discussed some baseline principles for the safeguards that a Party should take into consideration in the implementation of the Chapter II procedural powers and in Chapter III mutual assistance and cooperation.[40] These safeguards include the concept of "proportionality" in Article 15. This concept will fairly obviously vary depending on the Party concerned. "Proportionality" may require that a Party must put in place legislation to control the exercise of the power or procedure, so that it is proportional to the nature and circumstances of the offence. It may also require appropriate justification for the use of one of the Chapter II powers, judicial or other supervision of the exercise of the power, limitations in time and scope and so on. The limitation on interception in Article 21 of the Cyber-Crime Convention, which is confined to a range of serious offences (as defined in national law), is an express example of this approach.

The Cyber-Crime Convention contains no requirement that a party should put in place measures to compensate service providers or others who may be the targets of the exercise of the Chapter II, Section 2 powers and who may thus have to incur expense and install additional equipment in order to comply.

However the CDPC has noted that the concept of "proportionality" in Article 15 also requires a Party to consider the public interest in the sound administration of justice and in particular, "the rights, responsibilities and legitimate interests" of third parties, including service providers, as a result of an investigation and where appropriate. to mitigate that impact. [41] Any such "mitigating measures" are thus left to national law.

5. Conclusion

The Cyber-Crime Convention is the first real attempt to create an international treaty which harmonises criminal law and procedure in the area of computer crime and computer related crime. As such, it is an important step on the way to a truly global approach to combating the problem of cyber-crime. While heavily influenced by European legal principles and European thinking on human rights and privacy, it has nevertheless left significant human rights and privacy issues to the national law of those Council of Europe members and others who sign it. However, this is perhaps understandable in a Convention which addresses cyber-crime, rather than human rights and privacy. Nevertheless the Cyber-Crime Convention cannot be implemented in a vacuum. Any Party which signs the Cyber-Crime Convention must consider the impact of the Cyber-Crime Convention on national legal principles of human rights law and privacy. It is, in that sense, regrettable that the Cyber-Crime Convention does not set a clearer baseline for the privacy and human rights principles applicable to the investigation of cyber-crime and to international cooperation in this area.

---

1 http://conventions.coe.int/treaty/E/projets/FinalCyberRapex.htm

2 Reported on http://www.silicon.com on 3 July 2001

3 The Philippines-based author of the "Love Bug" virus of May 2000 was identified as a result of international police cooperation, but could not be prosecuted under Philippines law because no relevant criminal offence covered his **conduct.** Similarly, Lee Ashurst was charged under the law of the United Arab Emirates with misusing the equipment of Etisalat, as there is no specific offence of unauthorised computer access in the United Arab Emirates. He now faces a

compensation claim of £646,000 (or A$1.8 million) as a result of a civil claim brought by Etisalat for compensation arising from damage caused by his actions. Reported on http://www.silicon.com3 July 2001.

4 These 43 member countries include European Union Member States, members of the European Economic Area, Switzerland and former Soviet bloc states, some of whom are intending entrants to the European Union. They are Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Turkey, Ukraine and the United Kingdom.

5 Council of Europe Press Release of 22.06.2001

6 Article 36(3) of the Cyber-Crime *Convention*

7 eCommerce Today, Issue 140 and 141. There are similar initiatives by the G8 group of the world's 7 leading industrial nations and Russia. At the G8 Tokyo meeting in mid-June 2001, the G8 Government Private Sector High Level Meeting on High-Tech Crime has considered various computer crime issues, such as data preservation and protection of e-commerce and threat assessment and prevention, as well as addressing illegal content such as child pornography: eCommerce Today issue 143 22 June 2001 on page 1.

8 See the optional requirement for "dishonest intent" in the offences created under Article 2 (illegal access)

9 Article 4 (damage, deletion, deterioration, alteration or suppression of computer data)

10 Ibid. at Footnote 1

11 Paragraph 38 Draft Explanatory Memorandum of the draft convention on cyber-crime.

12 Ibid.

13 Paragraph 48 – Draft Explanatory Memorandum to the draft convention on cyber-crime.

14 According to the CDPC "access" means entering the whole or any part of a computer system (defined in Article 1 (a) as meaning any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data). Access does not include the mere sending of an e-mail message or file to that system. Paragraph 46 – Draft Explanatory Memorandum, Ibid.

15 Paragraph 69 of the Draft Explanatory Memorandum Ibid.

16 Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of conditional access.

17 ETS number 178

18 COM2000/854.

19 The reservations appear at Article 9(4).

20 For Article 10(1) these are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Copyright Treaty and for Article 10(2) the International Convention for the Protection of Performance, Producers of Phonograms and Broadcasting Organisations (the Rome Convention), TRIPS and the WIPO Performances and Phonograms Treaty. The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty have not yet entered into force.

21 Paragraph 116 of the Draft Explanatory Memorandum, Ibid.

22 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market particularly at Article 12 where the service provider acts as a "mere conduit" for transmission of information or provision of access to the communication network.

23 For example it is difficult to conceptualise an attempt to commit the sort of criminal copyright infringement offences set out in s132 of the Copyright Act 1968, .

24 Corporations, associations and similar legal persons: Paragraph 124 of the Draft Explanatory Memorandum, Ibid.

25 Article 12(3) of the Cyber-Crime Convention

26 Paragraph 124 of the Draft Explanatory Memorandum, Ibid.

27 Paragraph 125 of the Draft Explanatory Memorandum, Ibid.

28 Paragraph 125 of the Draft Explanatory Memorandum, Ibid.

29 The definition appears at s6(1) of the *Privacy Act 1988* (inserted by the Privacy Amendment (Private Sector) Act

30 s7B(3) Privacy Act 1988 (inserted by the Privacy Amendment (Private Sector) Act 2000, to come into force on 21 December 2001).

31 s6D –s6E

32 From a speech by the Hon. Bob Debus, Attorney-General for NSW at a seminar of E-Mail Surveillance in the Workplace for the Communications Law Centre. The text of the speech is available online at http://www.oznetlaw.net/pdffiles/ag_speech.pdf

33 This Act regulates the use of overt video surveillance technology in the workplace and requires employers to give notice to employees of video surveillance.

34 Traffic data is defined in Article 1 of the Cyber-Crime Convention. It is data required to route a communication to its eventual destination which can be crucial to identify the author of the communication.

35 See "Negotiators Finalise International CyberCrime Treaty, But Disagreements Remain" *Dow Jones Business News* 22/06/2001; "Dark Side of Cybercrime Fight" *Financial Times* 10/05/2001

36 The Statute of the Council of Europe (Treaty No 1 : London, 5.V.1949) Articles 1 and 3

37 This guarantees an individual's right to privacy in their home and family life and in their correspondence. It also protects the exercise of this right, except as in accordance with law, where this "is necessary in a democratic society in the interests of national security, ... for the prevention of disorder or crime... or for the protection of the rights and freedoms of others." Article 8(2).

38 Established under European Union's Data Protection Directive (95/46/EC of 24 October 1995), it has the responsibility of advising the European Commission on European privacy issues.

39 These issues are discussed by the Article 29 Working Party of the European Commission in its Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-Crime, commenting on the 25th Draft of the Cyber-Crime Convention. They also called for breaches of privacy legislation to be criminalised, along with the Article 2-11 offences.

40 *Paragraph 145-148 of the Draft* Explanatory Memorandum. Ibid

41 Paragraph 148 of the Draft Explanatory Memorandum