Author(s): Jahankhani, Hamid.
Article title: Evaluation of cyber legislations: trading in the global cyber village.
Year of publication: 2007
Citation: Jahankhani, H. (2007) 'Evaluation of cyber legislations: trading in the global cyber village', Int. J. Electronic Security and Digital Forensics, 1 (1) 1-11.
Link to published version: http://dx.doi.org/10.1504/IJESDF.2007.013588
DOI: 10.1504/IJESDF.2007.013588

Evaluation of cyber legislations: trading in the global cyber village

Hamid Jahankhani

School of Computing and Technology,
University of East London,
University way,
London E16 2RD, UK
E-mail: Hamid.jahankhani@uel.ac.uk

Abstract: The menace of organised crime and terrorist activity grows ever more sophisticated as the ability to enter, control and destroy our electronic and security systems grows at an equivalent rate. Cyber-crime (organised criminal acts using microchip and software manipulation) is the world's biggest growth industry and is now costing an estimated $220 billion loss to organisations and individuals, every year. There are serious threats to nations, governments, corporations and the most vulnerable group of all, individuals. Cyber-crime combines the same methods of traditional crime identifying targets, using surveillance and psychological profiling but has added-in levels of duplicity in that the perpetrator need never actually be at the scene of the crime. Indeed the traditional idea of a criminal gang is meaningless in that the unit may exist but each member resides on a different continent and never needs to physically meet. The types of attack individuals face include confidence-trick telephone calls or actual encounters calculated to extract bank or personal details, computer spyware that opens on accessing the internet, enticing users with offers of non-existent free gifts while copying confidential files and programmes that can infiltrate networks, operating within them undetected, ultimately causing them to crash. Information and services provided on the internet which can be utilised by any person(s) with access bring to fore the concept of legislations. Thus cyber laws and legislations refers to those guidelines and regulations put in place to ensure that information and services so displayed and acquired on the internet meet a standard within the e-society. This paper aims to review these legislations and showcasing their impact and relevance to the society for which they are formulated. Finally, the question whether the current internet legislation is adequate to protect society is also raised.

Keywords: cyber legislations; e-commerce directive; hacking; virus; worms; cyber-crime; spam; online advertising; e-society; distance selling.

1 Introduction

Computers have found their way into all areas of business, industry, education and government. Increasingly far reaching information networks linking computers and databases provide important benefits, including greater staff productivity and a sharper competitive edge. The more that we expand the reach of our information networks, the more important network security becomes.

The business risk for a company engaged in technologically dependent business is normally greater than for one that is not. Business operations present a unique set of risks, including an increased reliance on technology and increased vulnerability to the rapid changes in technology. In addition, industry structures can erode rapidly because internet shopping facilitates price competition and transforms core business structures to promote distribution by mail and remote customer service. To address such challenges, a company or a certain organisation needs to develop an effective strategy. An effective strategy requires operational efficiency; within organisation's information systems, this means an emphasis on information security and controls. A cost-effective business internal control system should be designed and implemented toward the goal of reduced operating expenses and therefore increased profits. Reducing operating expenses and increasing profits are critical to the success, even the continued survival, of companies heavily engaged in business.

2 Cyber legislations

Many countries have a legal system which is a combination of different legal principles for example English Law, Roman Dutch law and customary laws. All these laws were promulgated with a view to apply in a society where only off-line transaction had taken place. Therefore the main problem in the present day is to test the old laws with novel situations that arise with the development of ICT. Cyber-crime includes criminal trespass, wilful destruction of property, theft of intellectual property, infringement of trademark rights, forgery, obscenity, child pornography, larceny (theft) etc.

2.1 Potential trade mark liabilities

- *Domain name*: when can a domain name infringe trade marks rights of another? In the usual course of events, legal disputes in relation to domain names can arise in; conflicting interest disputes, 'palming off' dispute, competitor disputes, 'Cyber squatting' or domain name hijacking and cyber griping or parody dispute.

- *Linking*: another trade mark and unfair competition problem on the internet can arise when a person makes a link to materials to which the person does not have rights. Linking from one website to another is a normal practice in the web since it eases surfing the web. There are two type of linking one is hypertext link which is a reference link to the current search and the other is deep linking (inline linking) which refers to linking to an internal page of another website bypassing the home page of it. Deep linking can lead to many problems. Violation of trade mark rights arises when such a link leads the web user to believe that a webpage belongs to a certain trade mark owner. The problem of infringement of trade marks rights arise when such link categorically or by inference suggest an authorised association between the linking and linked sites and thereby diverts consumers from the source or origin.

- *Framing*: framing is a method of transmitting third parties sites or website owner's sites into the viewer's site to allow users access to other sites. This mechanism is mainly used for advertising. Advertisements which appear in the framing site from third party sites would divert advertising revenue to the third party. Here the problem of trade marks arises as a user may think that the advertised goods are from the original web site. The user is still able to see the entire framed site using the scroll bar without knowing the different origins of subframes. Since the framed URL is not displayed, the viewer can be misled as to the source origin of the site. Thus, potential trade mark liability can be raised. Moreover, framing becomes problematic when used to replace margins, generally consisting of advertisements, of the framed site with margins of the framing site. This would divert advertising revenue derived by selling advertisements placed within framed site to the framing site.

- *Meta-tags*: meta-tags is a variety of terms (keywords), which are embedded in the HTML code of a webpage thus enabling internet search engines to match a website to carry out a prioritise search query and hence increase traffic. Legal issues arise as to whether trade marks used as meta-tags would amount to infringement of trade mark rights. Trade mark law protects the proprietary rights of the trademark owner while protecting the public from being misled.

- *Mouse trapping*: mouse trapping is a technique by disabling the browser's functional commands keys such as 'back' and 'exit' so that internet surfer faced a flood of advertisements from adult sites. It can be argued that such use of trade mark would damage trade mark owner's goodwill and reputation. Therefore, any act or practice carried out or engaged in the course of business that damage the goodwill or reputation of another's enterprise shall constitute an act of unfair competition.

- *Spam*: the problem that arises in relation to spam can be seen in different areas including making nuisance, infringement of trade mark law etc. One should also look to other areas of law such as Consumer Protection, Data Protection Law and European Directives such as Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In Australia, The Spam Act 2003 is in force as of 10th of April 2004 makes it illegal to send even one unsolicited commercial electronic message that meets any one of the categories below;

- message sent from Australia
- by senders who; are physically present in Australia; are organisations with central management and control (board meetings) in Australia
- to computers in Australia (including the recipient's personal computer)
- to recipients who read the message when they; are physically present in Australia; are organisations carrying on business in Australia.

2.2 Hacking

Hacking is the gaining of unauthorised access to computer systems for the purpose of stealing and corrupting data. Section 1 of the UK Computer Misuse Act 1990 states that a person is guilty of an offence if

1 causes a computer to perform any function with intent to secure access to any program or data held in any computer

2 the access that person intends to secure is unauthorised and

3 knows at the time when causing the computer to perform the function, (Akdeniz, 2000).

2.3 Dissemination of viruses

UK, Section 3 of the Computer Misuse Act 1990 covers deliberate introduction of viruses. Under that section, a crime is committed, if a person causes unauthorised modification of the contents of any computer in order to either impair its operation, prevent or hinder access to any program, data or impair the operation of a program. Under Sri Lankan legal system there is no special law to prevent such deliberate act. However, to seek legal remedy under the general law of the country one has to find whether such act is accidental (perhaps as a result of a virus being contained in a piece of public domain or shareware software legitimately placed on the bulletin board for downloading) or due to gross negligence or wilful intent.

2.4 Online advertising

Advertising is any paid form of non-personal communication of ideas or products in the media, internet in this case (Jobber, 2001).

Internet users generally dislike the idea of online advertising (Kotler, 2003) and as such companies, organisations intending to advertise product and/or service online require a cost-effective approach to achieve their advertising objectives.

This said online advertising growth is bound to remain on the increase (eMarketer, 2002) due to a combination of the following reasons:

1 Growth in internet users.

2 Increased broadband penetration.

3 Resolving online standards. Voluntary regulations are being introduced by the Interactive Advertising Board (IAB) to ensure the ease of buying interactive advertising.

4 More online buyers.

Online advertising may take various forms dependent on the objective of the advertising company. Adverts can take forms such as:

1 Banner ads, these are graphical images often times with text appearing on designated portions on a web page. They are the most widely used online advertising tool and require users to click on them to get the intended information. A fee is normally charged for putting banner ads on relevant websites.

2 Sponsorship, best located on well-targeted sites where they can offer relevant information or service. The sponsor pays for showing the content and in turn receives acknowledgement as the sponsor of that particular service on the website.

3 Microsite, this is a limited area on the web managed and paid for by an external advertiser or company. These are particularly relevant for companies selling low-interest products such as insurance. For example an insurance company can create a microsite on a used-car website and offer advice to buyers of used along with a good insurance deal.

4 Interstitials, these advertisements pop-up between changes on a website.

5 Alliance and affiliate program, when internet companies work together, they end up advertising each other.

6 Spam, though unconventional, but still a form of advertisement. They are unsolicited commercial e-mail used to advertise products and/or services.

- *Advertising standards*: the Committee of Advertising Practice (CAP) publishes and enforces the British Code of Advertising, Sales promotion and Direct Marketing for non-broadcast advertisements in the UK through the Advertising Standards Authority (ASA). These organisations are jointly responsible for monitoring advertisements in paid for online space. The Code came into effect on 4th of March 2003 and has eight main rules governed by the principle that advertisements must be legal, decent, honest and above all truthful.

  Where the Code is breached, these organisations rely on the negative publicity generated, the possible refusal of advertising space, and removal of trade incentives by other trade organisations as a punishment to the culprit. The positive effects of these standards are evident in the number of complaints regarding internet-based advertisements received by the ASA.

- *Advertising to minors*: a minor can be described as an individual who has not yet reached 18 years of age. The key principle(s) governing advertising to minors across the globe covers issues such as;

  All advertisements are to be presented such that children will see or hear it and shall not be offensive to them. Care must be taken to design and present advertisements to children because of their credulity and the impressions they make of it.

  Where children partake in the advertisement, care must be taken to ensure that dangerous acts or situations are not shown which may lead them or other children into such a situation that is not permitted.

- *Advertising of particular products*:
  - Tobacco: the UK's Tobacco Advertising and Promotion Act 2002 passed into law on 7th of November 2002. This act identifies a tobacco advertisement as whose purpose and/or effect promotes a tobacco product, which is a product consisting wholly or partly of tobacco and intended to be smoked, sniffed, sucked or chewed.

    The act makes it an offence for an individual to publish a tobacco advertisement in the course of business and the printing and distribution of tobacco advertisement in the UK. This act further grants enforcement and powers of entry to duly authorised officers of an enforcement authority to possess any such distribution as necessary for the purpose of the proper exercise of his functions under this act.
  - *Alcohol*: noticeably, the review of researches around the globe found that advertising had no influence on consumption and no impact whatsoever on either experimentation with alcohol or its abuse. Alcohol can thus be ascribed to be a product that its consumers already know its basic characteristics and does not require advertisement to boost consumption or addiction. Alcohol advertisements are only done to encourage brand loyalty, (British Medical Journal, 1998).
  - *Drugs*: the uncontrolled advertising of drugs and nutritional supplements on the internet poses a potential health hazard (British Medical Journal, 1998) with companies misusing the internet for uncontrolled distribution of untested drugs.

    Under European law the promotion and advertising of prescription drugs to the public is not allowed and the placing of information regarding a prescription medicine on an open-access site by a manufacturer or pharmacist could consist illegal advertising (Council of the European Communities Directive 92/28/EEC, 1992).

2.5 Distance selling regulations

Distance selling involves the sale of goods and services between businesses and consumers concluded via the following means: mail order, fax and telephone, e-mail, the internet and interactive television.

The Consumer Protection (Distance Selling) Regulation came into effect for UK customers on Oct 2000. It grants customers the right to;

1 Get clear information from the supplier prior to placing an order.

2 Receive clear written confirmation from the supplier after placing an order.

3 Cancel the contract within a period of seven days after receipt or placing the order. This period may be extended for up to three months if the supplier had failed initially to provide necessary information as stated earlier.

2.6 Data protection issues

According to 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, the following where passed into law (Jahankhani and Alexis, 2002).

Article 2 of the Directive makes applicable the following definitions among others:

1 A ‘user’ refers to any natural person engaged in private or business purposes via available electronic communication services.

2 ‘Traffic data’ means data processed for the purpose of the conveyance of a communication on an electronic communication network or for billing thereof.

3 ‘Location data’ refers to data processed within an electronic communication network that indicates the geographic position of the terminal equipment of the user.

Article 4 directs the provider of a publicly available electronic communication service to take appropriate technical and organisational measures to safeguard security of its services and in cases of security breach, to inform its subscribers of the risk, measures being taken, remedies and an indication of the liability costs involved.

Article 5 enjoins member states to maintain the confidentiality of communication and related traffic data by prohibiting listening, tapping, storage or other types of interception or surveillance by persons other than the users without the consent of the users concerned.

Article 6 ensures that traffic data processed and shared by the provider must be erased or made anonymous once the duration of the service rendered lapses.

Article 12 enjoins member states to ensure that subscribers are informed, free of charge, before inclusion of their personal data on any printed or electronic directory made available to the public or obtainable through directory enquiry services.

2.7 Defamation

Defamation is a tort consisting of making a false statement about a person that injures his reputation in the community, (Girasa, 2002). Defamation Act 1996 sufficiently covers this offence in UK. The elements generally required for defamation are,

1 a statement either in writing or oral

2 that is false

3 tending to hurt person’s reputation in the estimation of others and

4 communicate to a third person.

Question arises on the issue of electronic publication, which requires that the defamatory statement is made known to a person or persons other than the plaintiff himself/herself. Placing such a message on a public access computer system would constitute a publication, but suppose the message was sent by e-mail, intended only for the plaintiff, but sent in such a way that it would be accessible by others. Is this the equivalent of sending a letter in an unsealed envelope, where the defendant may not be liable on the basis that he could not reasonably anticipate that someone would read a letter in an envelope addressed to another? Given the growth of e-mails, it is a matter of time before this issue becomes controversial.

3 Online selling and contract structure

Online selling involves the buying and selling of products and services over the internet. Online selling accounts for one of the major uses that the internet as been put to over the years. It involves the disclosure of personal information by the customer and under the European Directive of Data Protection discussed above; the service provider is under obligation to ensure the security of all information so gathered.

The online contract between a potential customer and a service provider does not have to follow a particular structure.

Its structure is dependent on the designer of the web pages for the service provider, it only obeys some specific rules most of which have been discussed.

The online contract, being a contractual obligation between both parties, must adhere to some or the entire following structural pattern;

1 Must indicate clearly the quantity, value and/or description of products ordered. It should also indicate the full value of all services rendered.

2 It should spell out clearly its accordance with relevant laws for example, Children's Online Privacy Protection Act (COPPA) where the customer may be less than 13 years of age.

3 It should get relevant personal data from the customer such as name, contact phone number, e-mail address, delivery address, billing address, password if generated etc. It should ensure the transmission of the information through a Secured Sockets Layer (SSL) that encrypts the information.

4 It should allow the customer to choose a billing option such as credit card and ensure the confirmation of the information thus given.

5 Allow the customer to print a copy of such completed contract for record purposes.

3.1 Online shopping

An analysis of virtual transactions to this point indicates a high proportion of name brand items and low cost items being purchased (Pope-Davis and Twing, 1991) frequently purchased items on the internet to this point include travel services, newspaper and magazine publishing companies (Buck, 1996). This would seem to reflect the risk reduction methods of

1 brand loyalty and

2 reducing the amount at stake in a purchase situation by limiting cost.

The risks associated with the inability to inspect merchandise, with difficulty in returning or exchanging merchandise and with the shopping medium transfer easily as internet shopping is still a form of phone/mail order purchasing.

However, some elements of a virtual sales situation present unique risks to the traditional phone/mail order scenario. First, the online shopping involves the use of a new technology, both in the ordering process itself and in the security mechanisms used to secure the transmissions. The unfamiliarity of the technology and the uncertainly associated with anything new are important considerations of commercial

internet ventures. With lack of experience or available information and training, consumers may continue using the web simply to collect information and not to purchase.

In electronic commerce, the ability of companies to reduce perceived risk and the establishment of trust between consumers and merchants is critical for consumers to engage in a virtual transaction beyond an initial purchase. Trust can be achieved or forfeited at several stages of a transaction. Firstly, the quality of goods and services must be satisfactory. Secondly, the consumer must trust the manufacturer that the product or service will be delivered. Thirdly, the consumer must trust the server and the manufacturer with the credit card transaction. Fourthly, the consumer must trust the technology involved in establishing and maintaining security and privacy in the transaction. Finally, the consumer must trust that if the product is damaged, defective or unacceptable, the manufacturer will honour some form of return policy.

4 Treaty on cyber-crime

One of the consequences of the 11th September 2001 terrorists attack on the USA, was the signing on 23rd November of the same year the international Convention on Cyber-crime by the US and 29 other countries (Zdrojeski et al., 2002). This international treaty aims at enforcing the ability of these nations to combat computer crime.

Among the many facets of the mandate were the following:

1 *Criminalisation of certain computer activities*: The treaty mandates each signatory to legislate domestic laws that criminalise the commission of the following actions, among others, without authority:

   a The interception, by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer carrying such computer data.

   b The damaging, deletion, deterioration, alteration of computer data.

   c The causing of property loss to another by any input, alteration, deletion of computer data or any interference with the functioning of a computer system with the fraudulent intent of procuring, without a right, an economic benefit for oneself or for another.

2 *Corporate liability:* the treaty requires signatory nations to impose and adopt necessary measures and legislation that makes a corporate entity liable for lack of supervision of an individual acting under its authority, when such lack of supervision results in the commission of a crime under the convention for the benefit of the entity.

3 *Preservation and production of stored computer data*: the adoption of legislation enabling domestic authorities to order or obtain the expeditious preservation of computer data for a period of 90 renewable days, especially where the data is vulnerable to loss or modification.

4 *Mutual assistance*: the treaty serves as an agreement among the signatory nations to afford one another mutual assistance to the fullest extent possible for the purpose of investigations or proceedings. Mutual assistance is subject to conditions set by the requested party but it cannot refuse assistance based on the fact that it considers the offence committed a fiscal one.

That the internet needs governance and content regulation is of no debate. The issue of governmental self-regulation or user design approach by the internet industry has been widely debated across the globe. Most research work done on the issue had resolved on the appropriate use of coregulation, which is to involve a harmonisation of both governmental principles and that of the internet industry.

The impracticability of either organ going it alone is very obvious. In the case of government's self-regulation, internet content regulatory powers tend to weaken across national borders as already discussed, since different nations have differing concerns.

In the case of privatised policing organisations, derived from the internet industry, the acceptability of these organisations to act as judge and jury over the suitability or illegality of internet content is a violation of due process concepts enshrined in international and national guarantees around the world (Strossen, 1999).

5 Conclusions

Despite a plethora of internet related legislation, cyber-crime is still a growing stigma for the e-society. It is evident that internet usage requires laws and regulatory authorities, which should span across national boundaries and legal systems. It is of particular importance that children online should be given adequate protection, which can only be enforced by suitable legislation.

However, internet laws regulations should be designed to reflect national values for national issues and international values for international issues. Suitable organisations should be set up to ensure that online organisations should adhere to all legislations covering their operations where possible. Responsibility for developing, evaluating, enhancing and safeguarding the internet and its related activities should lie with the international digital community. It should also be the e-community's responsibility to dictate the need for and to specify the extend of required legislation, since they will be the ones directly affected by such legislation. Necessary evaluation frameworks should be developed to assess the suitability and applicability of new laws, acts and directives issued. Government and non-government bodies and organisations can only contribute in laying the foundations, developing the strategies and overseeing the developments in terms of compatibility with general policies and national and international legal frameworks. It is a challenge for the rapidly increasing global digital community, to specify, modify, dictate, evaluate and safeguard sound legislation that would allow for efficient and socially responsible use of the internet worked world.

Organisations are highly exposed to the vulnerabilities inherent in internet connectivity and the exposure increases every day as viruses become more virulent and users neglect to exercise ever-greater caution. Moving away from the internet is not an option for most organisations. Competitiveness demands an ever-increasing presence and therefore reliance, on all things electronic. But many organisations have grown much larger by using their reliance on the internet, as the face of business transactions has changed dramatically over the last generation.

References

Akdeniz, Y. (2001) 'Internet content regulation: UK Govt and the control of internet content', *Published on Computer Law and Security Report*, Vol. 17, No. 5.

British Medical Journal (1998) *Dangers of Advertising Drugs on the Internet*, 16 October.

Buck, S.P. (1996) 'Electronic commerce – would, could, and should you use current internet payment mechanisms?' *Internet Research*, Vol. 6, pp.5–18.

Children's Internet Protection Act of 2000 (CHIPA) (2003) 47 U.S.C. sections 254 (h) and (l) 2000.

Children's Online Privacy Protection Act of 1998 (COPPA) (2003) 15 U.S.C. sections 6501-6506 (1998).

Council of the European Communities (1992) 'Directive 92/28/EEC of 31st March 1992 on the advertising of medicinal products for human use', *Official Journal European Communities L113*, pp.13–18.

Cyber rights (1996) 'Letter from the Metropolitan Police to UK ISPs', Available at: www.cyber-rights.org/documents/themet.htm, August 1996, Accessed on May 2003.

eMarketer (2002) 'Advertising spending', Available at: www.eMarketer.com. Accessed on. April 2003.

Girasa, R.J. (2002) *Cyberlaw, National and International Perspectives*, New Jersey, USA: Pearson Education Inc.

Jahankhani, H. and Alexis, S.A. (2002) 'E-commerce business practices in the EU', *International Conference on Enterprise Information Systems, ICEIS 2002*, Enterprise Information Systems IV, Kluwer Academic Publishers, pp.268–276, ISBN 1402010869.

Jobber, D. (2001) *Principles and Practice of Marketing*, 3rd edition, UK: McGrawHill.

Kotler, P. (2003) *Marketing Management*, 11th edition, UK: Prentice Hall.

Pope-Davis, D.B. and Twing, J.S. (1991) 'The effects of age, gender, and experience on measures of attitude regarding computers', *Computers in Human Behaviour*, Vol. 7, No. 4, pp.333–339.

Sarkar, P.K. and Cybulski, J.L. (2002) 'Understanding a product line of electronic business systems', Working Paper 2002/17, School of Information Systems, Deakin University.

Strossen, N. (1999) *ACLU Joins Protest Against Global Internet Censorship Plans* ACLU Press Release, 9 September.

Zdrojeski, R.W., Hoffman, L.D. and Dames, J. (2002) 'United States signs treaty on cyber-crime', *Internet Law Journal*, Available at: www.internetlawjournal.com.