Anonymity in Cyberspace: Finding the Balance between Privacy and Security

By

Mohamed CHAWKI

About the Author:

Mohamed Chawki (LL.B), (BA), (LL.M), (DU), (FRSA) is a "Junior Judge" at the Council of State (Conseil d'Etat), a Phd Researcher in cyberlaw at the School of Law, University of Lyon III, France; an expert in cybercrime at the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC); a fellow of the Royal Society of Arts in the United Kingdom (FRSA) and a member of Cybercrime Institute in France. Mohamed Chawki has taught part-time on Cybercrime and Cyberlaw for the LL.M English programme at the ITI Institute. He has authored many articles in English and French journals and conference papers. He is recipient of numerous academic prizes and the Medal of Excellence in 1998.

ABSTRACT

Anonymity in cyberspace is a major concern for the global community. The introduction, growth and utilisation of information and communication technologies (ICTs) have been accompanied by an increase in criminal activities. With respect to cyberspace, identities are easily cloaked in anonymity. Once a message sender's identity is anonymous, cyberspace provides the means to perpetrate wide spread criminal activity to the masses, with little chance of apprehension. On the other hand, anonymity in cyberspace allows whistle-blowers and political activists to express opinions critical of employers and the government enables entrepreneurs to acquire and share technical information without alerting their competitors, and permits individuals to express their views online without fear of reprisals and public hostility. On this basis the question of whether a State or a government can create a narrowly-tailored restriction on cyberspace anonymity without violating the privacy remains unresolved. Accordingly, this paper seeks to address and analyse the following issues. Firstly, it starts by presenting the concept and several types of anonymity. Secondly, it focuses on the Internet and how it can be achieved, and why it is an essential tool for free speech. The paper will also describe proposals to outlaw anonymity over the Internet, since it has often been tied to criminal activity by law enforcement bodies. Finally, the paper concludes that total anonymity may be possible through the use of privacy-enhancing technologies such as those offered by Anonymizer.com and Freenet. Moreover, educated legislators can criminalize most true anonymity in cyberspace and still pass security.

Keywords: Anonymity- Cybercrime – Cyberspace – Privacy

"While the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behaviour"

Former U.S. Attorney General Janet Reno, Jan. 10, 2000.

INTRODUCION

Anonymity[1] often considered a cornerstone of democracy and a First Amendment guarantee, is easier to attain than ever before, due to the recent emergence of cyberspace.[2] Cyberspace [3] allows people to share ideas over great distances and engage in the creation of an entirely new, diverse, and chaotic democracy, free from geographic and physical constraints. [4] As of September 2002, more than 182. 67 million adults had access to cyberspace in the United States and Canada, [5] and over 605.60 million had access worldwide. Those numbers are growing rapidly. Due to the nature of ICTs, identities[6] in cyberspace are easily cloaked in anonymity.[7] With this anonymity, cyberspace provides the means to perpetrate wide spread

[1] Anonymity is derived from the greek word **ανωνυμία**, meaning without a name or name-less. In colloquial use, the term typically refers to a person, and often means that the personal identity, or personally identifiable information of that person is not known. More strictly, and in reference to an arbitrary element (e.g. a human, an object, a computer), within a well-defined set (called the "anonymity set"), "anonymity" of that element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous".

[2] *See* G. du PONT, *The Criminalization of True Anonymity in Cyberspace*, (7 MICH, TELECOMM TECH. L. REV. 191), [2001].

[3] In fact, the term cyberspace literally means 'navigable space' and is derived from the Greek word *kyber* (to navigate). In William Gibson's 1984 novel, the original source of the term, cyberspace refers to, a navigable, digital space of networked computers accessible from computer consoles, a visual, colourful, electronic, Cartesian datascape known as 'The Matrix' where companies and individuals interact with, and trade in, information. Since the publication of this novel, the term cyberspace has been re-appropriated, adapted and used in a variety of ways, by many different constituencies, all of which refer in some way to emerging computer-mediated communication and virtual reality technologies. Here, we refocus the definition back to the envisaged by Gibson, so that cyberspace refers to the *conceptual space* within ICTs, rather than the technology itself. *See* W. GIBSON, *Neuromancer* (New York, Grafton), [1984]; M. DODGE, *Mapping Cyberspace* (N.Y, Routeldge), [2001] p. 1; D. PARKER, *Fighting Computer Crime* (N.Y., Wiley), [1998].

[4] *See* G. du PONT, *op. cit.*

[5] *See* <http://www.nua.org/surveys/how_many_online/index.html> (visited 03/01/2006).

[6] The term "identity" is commonly used arbitrarily and imprecisely in popular media and literature and the terms "identity theft" and "identity crime" are frequently used interchangeably. Occasional misusers are not surprising because in the contemporary context, the traditional meaning underlying those concepts have become increasingly known as information and information technology (IT). The *Oxford English Dictionary* defines "identity" as "*the set of behavioral or personal characteristics by which an individual is recognised*". The traditional use of the word "identity" spoke to one's name, familial membership and occupation. The contemporary meaning of "identity" has, however, assumed a candidly IT connotation that extends traditional meanings to include such things as one's consumer and credit histories, financial accounts, and Social security number. It is this contemporary usage of "identity" that is at issue when it comes to conceptualizing identity theft. *See* J. COLLINS, *Preventing Identity Theft Into Your Business* (New Jersey, John Wiley), [2005], p. 7; J. MAY, *Preventing Identity Theft* (N.Y., Security Resources Unlimited), [2004]; G. NEWMAN, *Identity theft* (U.S. Department of Justice, COPS), [June 2004], p. 7.

[7] *See* G. du PONT, *op. cit.* P. 192.

criminal activities with little chance of apprehension.[8] Reacting to several attacks on eBAY, CNN and other web sites, [9] former President CLINTON underscored the opinion that the government needs to maintain a watchful eye on cyberspace. [10] On the other hand, anonymity in cyberspace allows whistle-blowers and political activists to express opinions critical of employers and the government enables entrepreneurs to acquire and share technical information without alerting their competitors,[11] and permits individuals to express their views online without fear of reprisals and public hostility.[12] It is clear that in various parts of the world people may have an interest in not being identified and thus connected to certain published views and opinions.[13] Due to the international character of the Internet, those reasons for anonymous communications which are related to the "freedom of expression" may gain new dimensions.[14]

Before the information age, a person's identity, and information[15] relating to his or her identification seemed to be more precisely controlled.[16] But all that has changed. The advent of the information society has vastly increased the need for identifying mechanisms and thus public availability of the relevant technologies. [17] Names, addresses, e-mail addresses, photographs, social security numbers, etc., are freely available on the Internet and numerous identity related characteristics are for sale.[18] On the Internet, any one has the opportunity to gain knowledge about other people. The development of ICTs makes more and more people reluctant to reveal their true identity.[19] In combination with this, different services have recently been developed which make Internet activities, such as surfing anonymous.[20] Facilities are also anonymous. Facilities are also available to provide individuals with a pseudo identity.[21] Hence, anonymous communication is promoted as the solution to the

[8] *See Ibid;* M. GOODMAN and S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace* (U.C.L.A J. L. & TECH.), [2002], 3, 4-6.
[9] *See* E. HENSEN and J. BORLAND, *New Assault Weapons Pose Threat to Web*, available at CentNews.com
[10] *See* Clinton Taking up Web Security, available at: <http://66.249.93.104/search?q=cache:iusHg2nbJjsJ:amarillo.com> (visited 05/01/2006).
[11] *See* A. LEPAGE, *Libertés et Droits Fondamentaux à l'Epreuve de l'Internent* (Paris, Litec – édit du Juris Classeur), [2002], B. LAMY, *La Liberté d'Opinion et le Droit Pénal* (Paris, L.G.D.J), [2000].
[12] *See The Demise of Anonymity, A Constitutional Challenge to the Convention on Cybercrime* (LOYOLA OF LOS ANGELES ENTERTAINEMENT LAW REVIEW [Vol. 23:81], p. 82.
[13] *See* C. NICOLL, *Digital Anonymity and Law: Tensions and Dimensions* (The Hague, The Netherlands), [2003], p. 2.
[14] *See* J. LIPSCHULTZ, *Free Expression in the Age of the Internet: Social and Legal Boundaries* (Oxford, West View Press), [2000].
[15] According to the American Heritage Dictionary of the English Language, information is "knowledge of specific events or situations that has been gathered or received by communication, intelligence, or news".
[16] *See* C. NICOLI, *op. cit.* p. 3.
[17] *Ibid.*
[18] *Ibid* , C. VIER, *L'Internet et le Droit* (Paris, Victoires), [2001].
[19] *See* C. NICOLI, *op. cit.* p. 3.
[20] *See* M. BARKARDJIEVA, *Internet Society: The Internet in Everyday Life* (Sage Publishers), [2005].
[21] *Ibid.*

problem. However, anonymous raises various legal questions: What exactly do we mean by anonymity? Why would people want to communicate and transact on an anonymous basis? What are the practical and legal constraints upon anonymity when communicating and transacting with others? Finally, total anonymity may be possible through the use of privacy-enhancing technologies.[22]

1-ANONYMITY IN CYBERSPACE

There are actually two types of anonymity: true and pseudo-anonymity.[23] However, many scholars fail to address the distinction between these types. In this article, we will distinguish between true and pseudo – anonymity, two completely different forms of expression, with differing degrees of political and social values.[24]

1.1 True Anonymity

This kind of anonymity is untraceable. Indeed, only coincidence or purposeful self-exposure will bring the identity of the mystery sender to others; the identity of a person acting in a truly anonymous manner can not be definitively discovered through any amount of diligence. [25] Some attempts can be made to discover the identity of the sender through inference, but any concrete trail of clues betraying the message sender has been erased by circumstance, the passage of time, or by the sender himself. Although some forms of truly anonymous communication, such as political speech, are considered valuable, this form of anonymity has exceptional potential for illegal acts because the message senders cannot be held accountable for their actions.[26]

1.2 Pseudo-Anonymity

In this kind of anonymity, communications are inherently traceable.[27] Though the identity of the message sender may seem truly anonymous because it is not easily uncovered or made readily available by definition, it is possible to discover the identity of the pseudo-anonymous message sender. This kind of anonymity has significant benefits; it enables citizens of a

[22] A. BERTRAND : Droit à la Vie Privée et Droit à l'Image (Paris, Litec), [1999].

[23] *See* G. PONT, *The Criminalization of True Anonymity in Cyberspace* (7 MICH TELECOM TECH. L. REV. 191), [2001], p. 192.
[24] *Ibid.*
[25] *Ibid.*
[26] *Ibid.*
[27] *See* G. PONT, *op. cit.*

democracy to voice their opinions without fear of retaliation against their personal reputations, but it forces them to take ultimate responsibility for their actions should the need somehow arise.[28] Although governments could misuse their ability to uncover the identity of people acting pseudo – anonymously, it is not in the government's interest to break that trust; by respecting pseudo-anonymous identities, governments can often avoid the far more dangerous abuses stemming from true anonymity. [29]

2-ANONYMITY, PRIVACY AND FREEDOM OF SPEECH

Anonymity is important for on line discussions involving sexual abuse, minority issues, harassment, sex lives, and many other things.[30] Anonymity is also useful for people who want to ask technical questions that they don't want to admit they don't know the answer to, report illegal activities without fear of retribution, and many other things.[31] Without anonymity, these actions can result in public ridicule or censure, physical injury, loss of employment or status, and in some cases, even legal action. Protection from harm[32] resulting from this type of social intolerance is a definite example of an important and legitimate use of anonymity on the internet. An example of how vital such anonymity can be is exemplified by the following excerpt from a newsgroup post during a temporary shutdown of penet.fi:[33]

> "I had been posting to a non-technical *misc* newsgroup about an intimate topic for which I felt I required privacy. I have received immeasurable help from the people in that news group...Please, folks, believe me, I *need* this service. Please consider my point of view and permit admin@penet.fi to turn the service back on."

On such a basis, it is important to express certain opinions without revealing our true identities. Anonymity allows an individual to seek online information, resources and support without jeopardizing their public reputation and relationships. Fear of discrimination might prevent an individual from seeking help. Anonymity allows information gathering about issues like addictions to alcohol, gambling, drugs or sex; sexual identity, where identifying as

[28] *Ibid.*
[29] *Ibid.*
[30] *See* for example Doe v. 2 TheMart .com, Inc., 140F. Supp. 2d 1088, 1097 (W.D. Wash 2001); see also ACLU v. Miller, 977 F. Supp. 1228, 1232 (N.D. Ga 1997).
[31] For example, the state of Florida maintains an anonymous hotline for government workers to report wastes and abuses to the comptroller's office.
[32] *See* E.BERNARD, *The Collapse of the Harm Principle*, 90 (J. CRIM. L. & Criminology) 109, 120-39 [1999].
[33] *See* K. RIGBY, *op. cit.*

non-heterosexual could cause problems at work or home; testing or treatment options for illnesses like AIDS; or information about birth control or sexually transmitted infections. Anonymity is effective in promoting freedom of expression. Julf Helsingius asserts that anonymity is beneficial because it gives people an outlet for their opinions, even controversial ones. He argues that it is " *good to bring out things like that in daylight because that actually allows you to start processing it, see how people react to it, and so on*".[34] This may have sort of a cathartic effect in that it allows people to get their feelings out without physically hurting people of other cultures, races, etc. Moreover, anonymity hinders some methods of controlling the actions of other people. This is an additional argument in the usefulness of anonymity in the protection of freedom of expression. There are many long-standing precedents for anonymity in publishing. The responsibility of a journalist not to reveal their sources is recognized almost universally. Many authors write under pen-names and there are still some cases where the true identity of the author has never been discovered. Even the Federalist Papers were published under a pseudonym. Most newspapers publish letters to the editor and help columns and allow the letters to be anonymous or signed with a pseudonym and many newspaper articles are merely credited to "AP Newswire". Additionally, anonymous peer reviews of proposals and articles are common in academic circles.[35]

In *Forensic Advisors v. Matrixx Initiatives,* [36] a Maryland Court has been asked to order the disclosure of the identity of subscribers to a newsletter. In this affair, Matrixx, a pharmaceutical company was seeking a publisher's subscriber list to use in connection with a lawsuit filed against numerous individuals who posted allegedly derogatory comments about the company to an Internet discussion board.[37] Privacy and civil liberties advocates including EPIC, the Electronic Privacy Information Center have filed an amicus brief in support of the publisher's right to protect the list.[38] The brief argues that the list ought to be protected under Maryland law that protects a journalist's sources. They further argue that subscribers have a right to remain anonymous under the U.S. Constitution's First Amendment, since disclosure of the list would deter readership and violate established privacy rights. In *ACLU v. Miller* , [39] the American Civil Liberties Union got an injunction against the enforcement of a Georgia statute that prohibited a person from falsely identifying herself while sending e-mail, posting

[34] *See* K. RIGBY, *op. cit.*
[35] *Ibid.*
[36] *See Forensic Advisors v. Matrixx Initiatives* available at <http://www.epic.org> (visited 15/02/2006).
[37] *Ibid.*
[38] *See* S. KAKYTL, *Privacy vs. Privacy*, Yale Journal of Law and Technology, [Winter 2004],
[39] *See* <http://cyber.law.harvard.edu/> (visited 15/02/2006).

on the Internet, and more (one of the problems with the statute was that it was too vague). The court ruled it was appropriate to give an injunction, among other reasons, when there was the potential for chilling free expression. The court agreed with the state that its purpose in enacting the statute--preventing fraud--was a compelling state interest, but decided against the state because the statute was not narrowly-enough tailored to its purpose.[40] Finally, anonymous communication can be achieved in real life by sending an unsigned letter or making an anonymous phone call. From the large number of users who take advantage of anonymous services on the internet, it can be seen that these services are truly necessary and fill a specific need. The availability of the technology to set up such an anonymous server also makes the elimination of such servers virtually impossible; as soon as one is shut down, another one is created. The current availability of such services eliminates the need to forge an identity or use another person's identity to correspond anonymously. People on the net are anonymous to some degree anyway because of the inherent characteristics of the medium. Services providing additional anonymity are only expanding on this feature of the net. Pseudonymity comes in useful in that it allows users to send mail to pseudonymous users in response to their mail or post. People are able to respond to emails that they like or dislike or that they find offensive or disruptive. This makes the pseudonymous user more responsible for his or her actions than the completely anonymous user. They are still accountable for their actions on the net but are protected from "real world" damage.

Abolishing anonymity servers is not necessary since the technology exists to produce kill files which allow users to choose for themselves what they consider offensive. This allows individuals to filter out anonymous posts and emails which they dislike, while still reaping the benefits afforded by anonymous services. Although some people will automatically discount any anonymous postings, other people don't care who wrote it, as long as it is intelligent or funny. Still others use anonymity specifically to allow their opinions to be judged on their merit, rather than by the name attached to them.

3-IMPACT AND HARM GENERATED BY ANONYMITY

Although anonymity is extremely important for the protection of human rights, it is also tied with cybercrimes, or it is claimed that it would allow criminals to use the Internet without the

[40] *Ibid.*

possibility of detection.[41] With respect to cyberspace, identifying an electronic crime scene can be a daunting task when the perpetrator may have routed his communications with the victim through computers in three or four countries, with obscure networks that are inaccessible to investigators. Additionally, perpetrators could make things much more difficult and complicated by using technology and encryption techniques that provide a high-level of anonymity or assuming the identity of an innocent person. Moreover, the scale of cybercrime can exceed that of real-world crime in terms of the degree of harm[42] inflicted by a single crime.[43]

Criminals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive and potentially anonymous way to commit unlawful

[41] *See* Y. AKDENIZ, *Anonymity, Democracy and Cyberspace* (Social Research), Vol. 69, N°1 (Spring 2002), p. 5; M. WASIK, *Crime and the Computer* (Oxford, Rendon Press Oxford), [1998], A. LUCAS, J. DEVEZE and J. FRAYSSINET, *Droit de l'Informatique et de l'Internet* (Paris, PUF), [2001].

[42] The principle that the only justification for criminalizing conduct is to prevent harm is traceable in the writings of John Stuart Mill. In *On Liberty*, Mill declared that the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. J. MILL ON LIBERTY 9 (1859). The position Mill takes in this passage, of course, can only be used to justify the articulation of crimes against persons and crimes against property, for only these crimes directly inflict harm upon others. In the years after the appearance of On Liberty, Mills and later scholars expanded the principle so it now reaches a wide variety of harms. *See*, e.g., E.BERNARD, *The Collapse of the Harm Principle*, 90 (J. CRIM. L. & Criminology) 109, 120-39 [1999]. *See* also J. HALL, General Principals in Criminal Law 213-22 (1960). The nature of the harm encompassed by a criminal prohibition is not relevant to the issues under consideration in this article; the issue addressed in the section immediately above is whether or not the varieties of conduct that are currently, and casually, described as cybercrime result in the infliction of socially-intolerable harms that are distinct from those addressed by the repertoire of crimes respectively found in contemporary human societies. *See* also A.-C. DANA, *Essai Sur la Notion d'Infraction Pénale* (Paris, L.G.D.J.), [1982] ; C. MASCALA, *Droit Pénal Général* (Paris, Montchrestien), [2003] ; E. GARCON : Code Pénal Annoté (Paris, Sirey), [1956] ; J. LARGUIER : Droit Pénal des Affaires (8e éd. Colin.), [1992] ; A. AMIN, *Criminal Law* (Cairo, Lagna'at al Targama), [1923] ; H. Al-MARSAFAWI, *Criminal Law* (Alexandria, Al Ma'aref), [1991]; M. HOSSNI, *Special Criminal Law* (Cairo, Dar Al Naha Al Arabia), [1986]; M. MOUSTAFA : Droit Pénal Spécial (Cairo, Dar Al-Nahda Al-Arabia), [1984].

[43] There have been surveys of the incidence and effects of cybercrime on business. *See, e.g.*, U.S. Department of Justice – Bureau of Justice Statistics, Cybercrime Against Businesses [2004] at : <http://www.ojp.usdoj.gov/bjs/pub/pdf/cb.pdf> (last visited Sept. 27, 2004); Computer Security Institute, Ninth Annual CSI/FBI Computer Crime and Security Survey [2004] at : <http://www.gocsi.com/forms/fbi/pdf.jhtml> (last visited Sept. 27, 2004) [Hereinafter CSI/FBI Survey]; Australian CERT, 2004 Australian Computer Crime and Security Survey, at <http://www.auscert.org.au/> (last visited Sept. 18, 2004). These surveys generally do not differentiate between crime and cybercrime as *legal* phenomena. The question used in the Bureau of Criminal Justice Statistics' 2001 survey of cybercrime against businesses, for example, asked about the following categories of security threats: embezzlement; fraud theft of proprietary information; denial of service; vandalism or sabotage (electronic); computer virus, other intrusion or breach of computer systems, misuse of computers by employees, unlicensed use of copying of digital products developed for resale, and other.
See U.S. Department of Justice – Bureau of Justice Statistics, 2001 Computer Security Survey 1, *at* <http://www.census.gov/eos/www/css/cssprimary.pdf> (last visited Sept. 27, 2004). The same agency's survey of cybercrime cases handled by state prosecutors audited the following issues: credit card fraud, bank card fraud, computer forgery, computer sabotage, unauthorized access to computer, unauthorized copying or distribution of computer programs, cyberstalking, theft of intellectual property, transmitting child pornography, and identity theft. The CSI/FBI Computer Crime survey focused on these issues: virus insider abuse of net access, laptop/mobile theft, unauthorized access to information, system penetration, denial of service, theft of proprietary information, sabotage, financial fraud, telecom fraud. CSI/FBI Survey, as § II explains, these categories do not represent increments of a new type of criminal activity: cybercrime. Instead, they represent the use of computer technology to commit traditional offenses: crime. Section II considers whether the use of computer technology to commit crimes differs from traditional criminal activity in ways that justify treating it differently for purposes of legal analysis and/or tracking its incidence and effects; M. ERBSCHLOE, *Trojans, Worms and Spyware* (Oxford, Heinmann), [2005], p. 21.

acts, such as fraud,[44] the sale or distribution of child pornography, the sell of guns or drugs or other regulated substances without regulatory protections and the unlawful distribution of computer software or other creative material protected by intellectual property rights.[45] For example, some services like anonymous re-mailers can plainly frustrate legitimate law enforcement efforts despite providing privacy and encouraging freedom of expression. In the first case to be prosecuted in Queensland, a woman received e-mail correspondence that began amicably, but then became more threatening once she sought to end the communications.[46] She ultimately received death threats from the offender and threats to have her pack raped, videotaped and uploaded on the Internet.[47] In another case brought to court in United States, a University student harassed five female students after buying information about them via the net. The student sent over one hundred messages including death threats, graphic sexual descriptions and references to their daily activities.[48]

In another recent case, a phisher [49] e-mail claiming to be from MSN was sent to computer users. It said: "*we regret to inform you that technical difficulties arose with our recent update. Unfortunately part of our customer data base and back up system became inactive*".[50] This authentic-looking message offered a toll free telephone number in addition to a web link and urged individuals to click on the link to the phony web site. The message then informed individuals that they needed to enter their personal information. Later on, they realized that they were victims to this phishing attack.

Thus, territorial-based strategies tend not to be effective against online anonymity because they are designed to prevent the citizens of one nation-state from preying on each other, not to prevent their preying on citizens of other nation-states.[51] In this respect, Marc GOODMAN has succinctly stated:[52]

---

[44] *See* R. GELMAN, *Protecting Yourself Online, The Definitive Resource on Safety, Freedom and Privacy in Cyberspace* (Harpcollins Publishers), [1998].

[45] The Electronic Frontier [2000], also see R. SPINELLO, *Regulating Cyberspace: The Policies and Technologies of Control* (U.S.A, Spinello), [2002] p. 207; G. THERY, *Les Autoroutes de l'Information* (Report: La Documentation Française), [Octobre 1994].

[46] *See* E. OGILEIV, *The Internet and Cyberstalking*, available at <http://www.aic.gov.au> (visited 15/02/2006); P. SCHWARTZ, *Privacy and Democracy in Cyberspace* (52 VAND. L. REV 1609), [1999].

[47] *Ibid.*

[48] *Ibid.*

[49] The word phishing comes from the analogy that Internet scammers are using e-mail lures to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords from unsuspecting AOL users. Since hackers have a tendency to replacing "f" with "ph" the term phishing was derived. Available at <http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp> (visited 15/02/2006).

[50] *Ibid.*

[51] *See* S. BRENNER, *op. cit.* p. 19.

[52] *See* M. GOODMAN and S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace* (UCLA J. L. &

> [L]aw has evolved to maintain order *within* a society. Each nation-state is concerned with fulfilling its obligations to its citizens… [N]o nation can survive if its citizens are free to prey upon each other. But what if they prey upon citizens of *another* society? What if the citizens of Nation A use cyberspace to prey upon the citizens of Nations B and C? Is this a matter that is likely to be of great concern to Nation A? There are historical precedents for this type of behaviour that may shed some light on what will ensue in cyberspace. The most analogous involves high-seas piracy and intellectual piracy. Both involved instances in which societies were willing to allow (or even encourage) their citizens to steal from citizens of other societies. In both, the focus was on crimes against property the motivation was purely economic. [T]he conduct took place at the 'margins' of the law: high-seas piracy occurred outside the territorial boundaries of any nation and therefore outside the scope of any laws; eighteenth-century American intellectual property piracy [53]occurred when the legal status of intellectual property as 'property' was still evolving. Both were outlawed when they became economically disadvantageous for the host countries. One can, therefore, hypothesize that countries may be inclined to tolerate their citizens' victimizing citizens of other nations if (a) the conduct takes place at the margins of the law and (b) results in a benefit to the victimizing nation. The former gives the victimizing nation plausible deniability when confronted with its tolerance of illegal activity; the latter is an obvious motive for tolerating the activity.

Accordingly, law enforcement agencies are faced with the need to evaluate and to determine the source, typically on very short notice, of anonymous e-mails that contain bomb threats against a given building or threats to cause serious bodily injury.[54] Thus Internet based activities should consistently with physical world activities and in a technology-neutral way to further important societal goals (such as the deterrence and punishment of those who commit money laundering). National policies concerning anonymity and accountability on the Internet

---

TECH.), [2002], 3, 4-6.

[53] In 2002, Rep. Howard Berman introduced the Peer-to-Peer Piracy Prevention Act (2002), which would have protected copyright owners who engaged in acts of self-help to protect their works, H.R. 5211, 107th Cong. (2002), 18 U.S.C.A. § 1030; see also H. BERMAN, *The Truth About the Peer to Peer Piracy Prevention Act: Why Copyright Owner Self-help Must Be Part of the P2P Piracy Solution*, available at <http://writ.news.findlaw.com/> (visited 15/02/2006). During the summer of 2003, Senator Orrin Hatch proposed destroying the computers of individuals who illegally download material, pointing out that damaging someone's computer "may be the only way you can teach somebody about copyrights." Senator Takes Aim at Illegal Downloads, AP ONLINE, June 18, 2003 (on file with the Yale Journal of Law and Technology). Representative John Carter (R-TX) also suggested that jailing college students for piracy would deter other infringers. Katie Dean, Marking File Traders as Felons, Wired News, Mar. 19, 2003. In 2004, Congress considered the Inducing Infringement of Copyright Act of 2004, which aimed to hold software creators liable for the infringing activities of their consumers. *See* 2003 CONG US S. 2560, introduced [June 22, 2004] X. JARDIN Induce Act Draws Support, Venom, WIRED NEWS [Aug.26, 2004], at <http://www.wired.com/news/print/0,1294,64723,00.html> (visited 15/02/2006).

K . DEAN Copyright Proposal Induces Worry, Wired News [Sept.11, 2004] at http://www.wired.com/ news/politics/0,1283,64870,00.html; K. DEAN, Big Anti-Induce Campaig Planned, WIRED NEWS [Sept. 14, 2004] at : <http://www.wired.com/news/politics/ 0,1283,64935,00.html> (visited 15/02/2006).

Eventually the Induce Act was shelved, ostensibly due to the outcry among technology companies. *See* K. DEAN, Senate Shelves Induce Review, WIRED NEWS, [Oct. 7, 2004]

at <http://www.wired.com/news/politics/0,1283,65255,00.html>. Just a week later, however, former Attorney General John Ashcroft vowed to "build the strongest, most aggressive legal assault against intellectual property crime in our nation's history," *see* Katie DEAN, Ashcroft Vows Piracy Assault, Wired News, Oct. 14, 2004,

disponible at< http://www.wired.com/news/politics/ 0,1283,65331,00.html>.

[54] *See* S. LEVY, *Grand Theft Identity* (N.Y., Newsweek), [September 5, 2005), pp. 41.

thus need to be developed in a way that takes account of privacy, authentication, and public safety concerns.[55]

In one recent case, Judy McDonough, a 56-year-old occupational psychologist from Shaw, England, suffered a disturbing blow: she realized someone had stolen her identity from Internet.[56] But by that time, the thief had already opened two credit cards in her name, taken out three bank loans and ordered £ 2, 3000 in debt in three years.[57] McDonough tried six times to report the crime to the local authorities, and bank officers made lacklustre efforts to help. Finally, McDonough turned to her Member of Parliament for assistance. Hitherto the thief – who McDonough suspects is a relative-, has not been caught.[58] In another very recent case,[59] an American citizen tried to sell his house in California. He contacted several real estate agents to discuss with them a listing for the house. He was then informed by these agents that his house has been rented to individuals that he was not aware of or have even agreed to rent his house to. Someone was collecting the rent on his house, and upon checking with the USA county records he found out that someone has used his name and arranged to fake his signature, made a power of attorney in his name and received loans on his property, bought a business in his name and has accumulated a huge amount of financial burden in his name as well. The personal information of this victim was found and downloaded from Internet.

4- REGULATING ANONYMITY IN CYBERSPACE

From logical, theoretical, and pragmatic perspectives, knowing the problem, risks associated therewith, and the ills resulting there from is an indispensable step towards a possible regulation. Since these issues are difficult and sensitive, it is not easy to decide how to legally regulate anonymity in cyberspace. According to an EC report, published in 1999:[60] *" Users may wish to access data and browse anonymously so that their personal details cannot be recorded and used without their knowledge. Content providers on the Internet may wish to remain anonymous for legitimate purposes, such as where a victim of a sexual offence or a person suffering from a dependency such as alcohol or drugs, a disease or a disability wishes to share experiences with others without revealing their identity, or where a person wishes to*

[55] *Ibid.*
[56] *See* S. LEVY, *op. cit.*
[57] *Ibid.*
[58] *Ibid.*
[59] Privacy Rights Clearing House (UCAN), [Feb. 2005].
[60] *Ibid.*

report a crime without fear of retaliation. A user should not be required to justify anonymous use. Anonymity may however also be used by those engaged in illegal acts to complicate the task of the police in identifying and apprehending the person responsible. Further examination is required of the conditions under which measures to identify criminals for law enforcement purposes can be achieved in the same way as in the "off-line" world. Precedents exist in laws establishing conditions and procedures for tapping and listening into telephone calls. Anonymity should not be used as a cloak to protect criminals".

At the present time no consistent policy can be discerned in any one jurisdiction that would allow the resolution of the tensions illustrated above. Each problem relies on striking a faire balance between the interests of the individual on the one hand, and the interests of the State on the other. Various countries have laws both protecting and forbidding anonymity. For example, many countries have laws protecting the anonymity of a person giving tips to a newspaper, and laws protecting the anonymity in communication with priests, doctors, etc. [61] On the other hand, the obvious risk of misuse of anonymity has caused some countries to try special legislations concerning its regulation. [62] Cases of defamation often result in corporations seeking motions to uncover the identities of individuals who have made negative comments on bulletin boards or websites.[63] Although hurtful, these comments are often opinions, not facts and therefore not punishable crimes.[64] In the case of cyber-trespass, it is first required that plaintiffs show damages caused by defendants. Safeguards ensure that anonymity is protected until proof of a crime exists. These safeguards prevent an ISP from providing a "subscriber's personal information without the subscriber's knowledge and consent, except in certain specified circumstances. [65] Accordingly, the Council of European Union has adopted a Directive of the European Parliament and the Council on data retention[66], amending directive 2002/58/EC. The Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications service or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to insure that the data are

[61] *See* J. PALME and M. BERGLUND, *Anonymity on the Internet*, p. 4.
[62] *See* Three EU governments - UK, France and Belgium - press ahead with 12 months retention of telecommunications data - ditching citizens' rights on data protection and privacy under EU law. Available at: <http://www.statewatch.org/news/2001/may/03Genfolpol.htm> (visited 13/02/2006).
[63] *See* A. STILES, *Everyone's a Critic: Defamation and Anonymity on the Internet* [2002], Duke L. & Tech. Rev. 0004.
[64] *Ibid.*
[65] *See* M. HOMSI and A. KAPLAN – MYRTH, *Online Anonymity and John Doe Lawsuits*? [19 Jan 2005] University of Ottawa Canadian Internet Policy and Public Interest Clinic <http://www.cippic.ca/> (visited, 14 August 2005).
[66] Directive on Data Retention (2005/0182/COD); V. SQUARCIALUPI, *Lutte de l'Europe contre la Criminalité Economique et le Crime Organisé Transnational, Progrès ou Recul ?* (Conseil de l'Europe), [6 avril 2001].

available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

The Directive is applied to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not be applied to the content of electronic communications; including information consulted using an electronic communications network. The data retained are provided only to the competent national authorities in specific cases and in accordance with national law. They are retained for periods of not less than six months and not more than two years from the date of communication. "*Agreement on retaining communications data places a vital tool against terrorism and serious crime in the hands of law enforcement agencies across Europe* " British Home Secretary Charles Clarke said in a statement. Modern criminality crosses borders and seeks to exploit digital technology. [67] Member States have to take necessary measures to insure that any intentional access to, or transfer of; data retained is punishable by penalties, including administrative or criminal penalties that are effective, proportionate and dissuasive. Each Member State will designate a public authority to be responsible for monitoring the application within its territory of the provisions adopted regarding the security of sorted data.[68]

Following entry into force of the directive, Member States will have as a general rule 18 months in which to comply with its provisions.

At the same time, governments have confronted the dangers of cyberspace by devoting significant resources towards formulating a legal framework that addresses the technical and operational challenges of crime.[69] The Convention on Cybercrime is considered "*one of the most important legal instruments elaborated within the Council of Europe*". [70] It was approved by the Committee of Ministers of the Council of Europe (COE), and on November 23, 2001, the Convention was signed by twenty-six member states of the COE along with four non-member states — Canada, Japan, South Africa, and the United States, and entered into force on July 7, 2004.[71] The Convention is the first international treaty to allow police in one country to request that their counterparts abroad collect an individual's computer data, have the individual

[67] *See* EU Data Retention Directive Gets Final Nod, available at <http://news.com.com> (visited 03/03/2006).
[68] *See* N. FERQUSON, *Practical Cryptography* (N.Y., John Wiley), [2003], p. 8.
[69] *See* Aldesco, The Demise of Anonymity: A Constitutional Challenge to the Convention of Cybercrime, available at <http://elr.lls.edu/issues/v23-issue1/aldesco.pdf> (visited 05/03/2006).
[70] *Ibid.* See also S. HOPKINS, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead* (Journal of High Technology Law), [2004], p. 105.
[71] *See* Convention on Cybercrime, available at <http://conventions.coe.int> (visited 05/03/2006).

arrested and extradited to serve a prison sentence abroad.[72] It aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime; (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; (3) setting up a fast and effective regime of international co-operation. [73] The Convention defines substantive criminal laws to be legislatively adopted by all signatory states. It covers crimes in four main categories: (1) "offences against the confidentiality, integrity and availability of computer data and systems;" [74] (2) computer-related offences; [75] (3) content-related offences (for example, child pornography); [76] and (4) "offences related to infringements of copyright and related rights." [77]

The Convention also seeks to harmonize new procedures and rules of "mutual assistance" to aid law enforcement in the investigation of cybercrimes. Signatory countries are required to ensure that certain measures are available under their national law: "*[e]expedited preservation of stored computer data;*" expedited preservation and disclosure of traffic data; the ability to order a person to provide computer data and to order an ISP to provide subscriber data under its control; "[r]eal-time collection of traffic data;"[78] and interception of content data.[79] The Convention provides that signatory countries must adopt measures to establish jurisdiction over any offences committed in their respective territories or by their nationals.[80] Moreover, it empowers legal authorities and police in one country to collect evidence of cybercrimes for police in another country, and establishes a "24/7 network"[81] operating around the clock, seven days per week, to provide immediate assistance with ongoing investigations.

According to article 15 which deals with "conditions and safeguards," the "*establishment, implementation and application of the powers and procedures provided for in [Section 2 of the Convention pertaining to procedural law] are subject to conditions and safeguards*" provided

---

[72] *See generally* Mike Godwin, *International Treaty on Cybercrime Poses Burden on High-Tech Companies*, IP Worldwide [Apr. 4, 2001], *at* <http://www.law.com> (explaining that this treaty would permit extradition of computer users in other countries); see also S. BRENNER, *Cybercrime Metrics: Old Wine, New Bottles* (Virginia, Virginia Journal of Law and Technology), [2004].

[73] Council of Europe, Convention on Cybercrime, European Treaty Series (ETS) no. 185, *at:* <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

[74] Cybercrime Convention, arts. 2 – 6.

[75] Cybercrime Convention, arts. 7 – 8.

[76] *Ibid* art. 9.

[77] *Ibid* art. 10.

[78] *Ibid* art. 20.

[79] *Ibid* art. 21.

[80] *Ibid* art. 22.

[81] *Ibid* art. 35.

under the domestic law of each signatory country. These domestic laws and procedures shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure.[82] Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments.[83] These instruments include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005, 009, 046, 114, 117 and 177), in respect of European States that are Parties to them. It also includes other applicable human rights instruments in respect of States in other regions of the world (e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights) which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.[84]

Article 19 of this Convention aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings.[85] Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data *per se* will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored.[86] The aim of this article is to establish an equivalent power relating to stored data which is contained either within a computer system or part of it (such as a connected data storage device), or on an independent data storage medium (such as a CD-ROM or diskette).

To strike a balance between privacy and security in cyberspace, article 8 of the European

[82] *See* Convention on Cybercrime , Explanatory Report.
[83] *See* Convention on Cybercrime, Explanatory Report.
[84] *See* Convention on Cybercrime, Explanatory Report.
[85] Cybercrime Convention, art. 19.
[86] *Ibid.*

Convention on Human Rights and Fundamental Freedoms gives a right to *respect* for a citizen's private life, his home and his correspondence. But the flexible notion of "respect" is informed by the interests of national security, public safety, the economic well-being of the country, prevention of disorder and crime.[87] Protection of public morals and the rights and freedoms of others. In the U.S.A. for example, there is no express right to privacy guaranteed by the Constitution. There, the recognition of the need for citizens to be able to communicate anonymously is derived from the right to speak freely, to dissent and criticize.[88]

Clear guidelines seem only to exist in the political context. Commercial interests are accorded reduced protection. There is no equivalent of the express reference to the economic well-being of the country as exists in the European Convention on Human Rights and Fundamental Freedoms.[89] It may be that the market will regulate itself. That may be trough compromising or the "spending" of privacy which becomes tantamount to an asset. The countervailing benefit is some form of financial gain. The market may also regulate itself through a professional body or association. For example, Yahoo! has policies that allow it to reveal the identities of its users when the service provider is subpoenaed, subjected to court orders or involved in a legal process.[90] The fact that these companies can and will identify Internet users when asked by a court to do so forces courts to decide whether to protect the anonymity of Internet users sued for crimes or require their identity to be revealed in order to have a more easily administered crime lawsuit. But here, as illustrated by Carr, [91] in connection with the Internet Watch Foundation, a private association may effectively block the door to the Internet or restrict permissible activities in the absence of any public debate or even in direct opposition to public demand. The danger of this sort of private intervention is that it may often occur because the trade body concerned fears government regulation. The government is able to abdicate its responsibilities in a politically unproductive or dangerous area by permitting a form of delegated legislation while avoiding any accountability.[92]

Yet fundamental to the regulation of anonymous Internet activity is the recognition that communication is not "geographically contained". The nature of the medium dictates that the prevention of cybercrime for example, must be accompanied by a degree of international co-operation that has not so far been possible to attain in other contexts. Not only is it difficult,

[87] *See* C. NICOLL, *Digital Anonymity and the Law: Tensions and Dimensions* (NOW, the Hague), [2003], p. 294.
[88] *Ibid.*
[89] *Ibid.*
[90] *See* A. STILES, *op. cit.*
[91] *Ibid.*
[92] *See* C. NICOLL, *op. cit.* p. 295.

owing to political, cultural differences, to reach an international consensus on a list of alleged crimes that would justify a co-ordinated approach in their detection, but the process is further exacerbated by wide dissemination of evidence, the transient nature of much of the evidence and a trail that quickly turns cold. According to Sims,[93] various procedural means are available in common law countries to gain the courts' assistance in breaking through identity barriers. Yet these methods can be hampered by a lack of formalized transitional co-operation. The nature of cyberspace is not only a problem in securing a uniform approach to online-anonymity. Howells and Edwards argue that anonymity give an unfair advantage to lobby or interest groups who are able to band together and thereby to focus attention on influencing legal developments to their advantage at the expense of less cohesive or numerically manageable interests such as consumers. Ironically, it is consumers who are the major driving forces in the growth of e-commerce. Yet surveys have shown that they have little confidence in the medium, an attitude that is, perhaps, disproportionately affected by invasions of privacy such a spam and junk mail which, whilst they do little economic harm, can cause huge annoyance.

5 – THE CASE LAW

In the last few years, Internet libel suits involving anonymous statements have begun cropping up in courtrooms across the USA.[94] The two notable cases discussed below exhibit different approaches to solving the problems presented by anonymous libel on the Internet. One seems to provide a satisfying solution while the other creates practical problems that undermine the tort of defamation all together.[95]

Melvin v. Doe

In November 2000, the Court of Common Pleas of Allegheny County, PA, held that if the plaintiff could prove the identity of defendant was " *(1) material, relevant, and necessary, (2) cannot be obtained by alternative means, and (3) is crucial to plaintiff's case*," the First Amendment would not protect the anonymity of the defendant.[96] In *Melvin v. Doe*, an unknown person published statements on a website that accused a local judge of political

[93] *Ibid.*
[94] *See* A. STILES, *op. cit.*
[95] *Ibid.*
[96] *See* R. GASPAR, *Looking to the Future: Clarity on Communications Data Retention Law*, cited in *Ibid.*

activity that was inappropriate for a judge in her position.[97] The plaintiff sued the unknown speaker for defamation and tried to obtain his identity during discovery.[98] The defendant petitioned the court for a protective order that would prevent this discovery. However, the order was denied.[99] The court reasoned that a state's interest in discouraging defamatory statements about public officials by traditional media extended to statements made on the Internet. It held that because of this interest, there was no absolute immunity for Internet speakers with regard to the defamation tort.[100] The court then applied the three-part test discussed above to the request for the speaker's identity.[101] Without much discussion about the test's application to the specific facts of the case, the court held that the plaintiff's interest outweighed the defendant's, and the protective order should be denied.

The Ampex case

While the *Melvin* case was decided in 2000, more recently, a judge in California took a different approach to the Internet anonymity question.[102] The Contra Costa County Superior Court ruled that plaintiffs in libel actions must prove that the allegedly libellous statement is in fact libellous before the identity of the speaker will be revealed.[103] In this case, the plaintiff, *Ampex*, asked the judge to reveal the identity of an Internet speaker who posted anonymous messages about the company and its executives. *Ampex* claimed the messages were defamatory and said it needed the identity of the speaker so the lawsuit could proceed.[104] The judge rejected this request and gave *Ampex* a week to prove the statements were libellous before the plaintiff could obtain the speaker's identity.[105]

[97] Letter from J. ABBOTT, Director General, National Criminal Intelligence Service, to Guardian [June 15, 2000], cited *in Ibid.*
[98] *See* D. BLUNKETT, *Democracy Must Be Vigorously Defended*, Tribune, Oct. [26, 2001].
[99] Home Office, Retention of Communications Data.
[100] *See* P. HEWITT, Labour E – Minister, available at <http://www.politicalstalk.guardian.co.uk>.
[101] *See* <http://www.fipr.org>
[102] *See* A. STILES, *op. cit.*
[103] *Ibid.*
[104] *Ibid.*
[105] *Ibid.*

6 – CONCLUTIONS

This article aimed to explore and analyze anonymity in cyberspace. It shows that there is no definite guideline to determine the boundaries of anonymity and interests that determine whether and to what extent limitations on anonymity are required or not. It shows that limitations on anonymity could be said to reflect the legislator's recognition on various interests in making a person's identity known. Accordingly, one of the digital applications that could bring potential for balancing anonymity and the quest of governments and businesses to have identification data available is the facility of Trusted Third Parties; such as the Certification Authorities or anonymity software. These could play an intermediate role in keeping a true identity secret and also in providing identity and tracing information once certain conditions are satisfied. There will be always be a continued debate, such as in France, whether they must retain in escrow identifying information in the event that governments require to decrypt messages for state security reasons. In line with the present developments in the U.S.A. where Internet Service Providers have to reveal the identity of people posting information through their facilities, case law, self regulatory initiatives and maybe even legislation may set the conditions under which identifying information must be revealed by intermediaries.

BIBLIOGRAPHY

- English Books and Articles:

1. A. ALDESCO, *The Demise of Anonymity, A Constitutional Challenge to the Convention on Cybercrime* (Loyola of Los Angeles Entertainment Law Review), [vol. 23:81].
2. A. MICHAEL, *The Death of Privacy?* (52 STAN. L. REV. 1461), [2000].
3. A. STILES, *Everyone's a Critic: Defamation and Anonymity on the Internet* (Duke L. & Tech. Rev. 0004.), [2002].
4. C. NICOLL, *Digital Anonymity and Law: Tensions and Dimensions* (The Hague, The Netherlands), [2003].
5. D. BLUNKETT, *Democracy Must Be Vigorously Defended* (Tribune), [26 oct., 2001].

6. D. PARKER, *Fighting Computer Crime* (N.Y., Wiley), [1998].
7. E.BERNARD, *The Collapse of the Harm Principle*, 90 (J. CRIM. L. & Criminology) 109, 120-39 [1999].
8. E. HENSEN and J. BORLAND, *New Assault Weapons Pose Threat to Web*. Available at: <http://www.centnews.com> (visited 03/01/2006).
9. E. OGILEIV, *The Internet and Cyberstalking*, available at: <http://www.aic.gov.au> (visited 15/02/2006).
10. G. NEWMAN, *Identity theft* (U.S. Department of Justice, COPS), [June 2004].
11. G. PONT, *The Criminalization of True Anonymity in Cyberspace*, (7 Mich, Telecomm Tech. L. Rev. 191), [2001].
12. H. BERMAN, *The Truth About the Peer to Peer Piracy Prevention Act: Why Copyright Owner Self-help Must Be Part of the P2P Piracy Solution*, available at: <http://writ.news.findlaw.com/> (visited 15/02/2006).
13. J. ABBOTT, *Director General, National Criminal Intelligence Service* (Guardian), [June 15, 2000].
14. J. COLLINS, *Preventing Identity Theft Into Your Business* (New Jersey, John Wiley), [2005].
15. J. KANG, *Information Privacy in Cyberspace Transactions*, (50 STAN. L. REV. 1193, 1195-99), [1998].
16. J. LIPSCHULTZ, *Free Expression in the Age of the Internet: Social and Legal Boundaries* (Oxford, West View Press), [2000].
17. J. MAY, *Preventing Identity Theft* (N.Y., Security Resources Unlimited), [2004].
18. J. PALME and M. BERGLUND, *Anonymity on the Internet*, available at: <http://dsv.su.se/jpalme/society/anonymity.html> (visited 03/02/2006).
19. J. WALLACE, *Nameless in Cyberspace: Anonymity on the Internet* (Cato Institute), [1999].
20. K . D E A N , *Copyright Proposal Induces Worry*, Wired News [Sept.11, 2004], available at: <http://www.wired.com/> (visited 15/02/2006).
21. K. RIGBY, *Anonymity on the Internet Must be Protected* (Ethics and Law on the Electronic Frontier, [Fall 1995].
22. M. BARKARDJIEVA, *Internet Society: The Internet in Everyday Life* (Sage Publishers), [2005].
23. M. DODGE, *Mapping Cyberspace* (N.Y, Routeldge), [2001].

24. M. ERBSCHLOE, *Trojans, Worms and Spyware* (Oxford, Heinmann), [2005].
25. M. GODWIN, *International Treaty on Cybercrime Poses Burden on High-Tech Companies*. Available at: <http://www.law.com> (visited 05/04/2001).
26. M. GOODMAN and S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace* (U.C.L.A J. L. & Tech.), [2002], 3.
27. M. HOMSI and A. KAPLAN – MYRTH, *Online Anonymity and John Doe Lawsuits*? [19 Jan 2005] University of Ottawa, Canadian Internet Policy and Public Interest Clinic. Available at: <http://www.cippic.ca/> (visited, 14 August 2005).
28. M. WASIK, *Crime and the Computer* (Oxford, Rendon Press Oxford), [1998].
29. N. FERQUSON, *Practical Cryptography* (N.Y., John Wiley), [2003].
30. P. SCHWARTZ, *Privacy and Democracy in Cyberspace* (52 VAND. L. REV 1609), [1999].
31. R. GELMAN, *Protecting Yourself Online, The Definitive Resource on Safety, Freedom and Privacy in Cyberspace* (Harpcollins Publishers), [1998].
32. R. N'ŒIL, *The First Amendment and Civil Liability*, (Indiana, Indiana University Press), [2001].
33. R. SPINELLO, *Regulating Cyberspace: The Policies and Technologies of Control* (U.S.A, Spinello), [2002].
34. S. BRENNER, *Cybercrime Metrics: Old Wine, New Bottles* (Virginia, Virginia Journal of Law and Technology), [2004].
35. S. HOPKINS, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead* (Journal of High Technology Law), [2004].
36. S. KAKYTL, *Privacy vs. Privacy*, Yale Journal of Law and Technology, [Winter 2004].
37. S. LEVY, *Grand Theft Identity* (N.Y., Newsweek), [September 5, 2005].
38. Y. AKDENIZ, *Anonymity, Democracy and Cyberspace* (Social Research), vol. 69, n°1 [Spring 2002].
39. W. GIBSON, *Neuromancer* (N. Y., Grafton), [1984].

- French Books and Articles:

1. A.-C. DANA, *Essai Sur la Notion d'Infraction Pénale* (Paris, L.G.D.J.), [1982].
2. A. BERTRAND, *Droit à la Vie Privée et Droit à l'Image* (Paris, Litec), [1999].

3. A. LEPAGE, *Libertés et Droits Fondamentaux à l'Epreuve de l'Internent* (Paris, Litec – édit du Juris Classeur), [2002].
4. A. LUCAS, J. DEVEZE and J. FRAYSSINET, *Droit de l'Informatique et de l'Internet* (Paris, PUF), [2001].
5. B. LAMY, *La Liberté d'Opinion et le Droit Pénal* (Paris, L.G.D.J), [2000].
6. C. MASCALA, *Droit Pénal Général* (Paris, Montchrestien), [2003].
7. C. VIER, *L'Internet et le Droit* (Paris, Victoires), [2001].
8. E. GARCON, *Code Pénal Annoté* (Paris, Sirey), [1956].
9. F. SEMUR, *La Fraude Télématique* (Paris, Expertise), [novembre 1991].
10. G. ROMAIN, *La Délinquance Informatique : Où en Est-on ?* (Sécurité Informatique), [Juin 1998].
11. G. THERY, *Les Autoroutes de l'Information* (Report: La Documentation Française), [Octobre 1994].
12. J. HUET, *Quelle Culture dans le Cyber-Espace et quel Droits Intellectuel pour cette Cyber-Culture* (Paris, Chron.), [1998].
13. J. LARGUIER, *Droit Pénal des Affaires* (8e éd. Colin.), [1992].
14. V. SQUARCIALUPI, *Lutte de l'Europe contre la Criminalité Economique et le Crime Organisé Transnational, Progrès ou Recul ?* (Conseil de l'Europe), [6 avril 2001].

- Arabic Books and Articles:

1. A. AMIN, *Criminal Law* (Cairo, Lagna'at al Targama), [1923].
2. H. Al-MARSAFAWI, *Criminal Law* (Alexandria, Al Ma'aref), [1991].
3. M. HOSSNI, *Special Criminal Law* (Cairo, Dar Al Naha Al Arabia), [1986].
4. M. MOUSTAFA, *Special Criminal Law* (Cairo, Dar Al-Nahda Al-Arabia), [1984].