Global Information Assurance Certification Paper

System Security Liability

Does it always float downstream?

Eardley P. Grant
GIAC Security Essentials Certification Practical (GSEC)
August 2004
Practical Assignment Version 1.4b Option 1

Table of Contents

1.0 Introduction

1.1 Report Scope

This report is an evaluation and analysis of the potential threat posed by information systems negligence and liability suits to companies as well as individuals. While such liability suits are rare, there are strong indications from various regulatory bodies and judiciaries that the strict tort standard for establishing negligence will be easier to meet in the future.

This report will attempt to explain using case law and hypothetical examples in generic terms using research and interviews with Internet law experts on the implications of downstream liability. The notion of downstream liability while usually associated with commercial entities, can, and will probably be applied to private citizens with broadband connections. The fact that home users potentially can also be liable for downstream negligence, could affect the push by governments to commoditize broadband Internet access for its citizenship. This, if not addressed through prudent policy decisions and educational initiatives, could derail national policies on eGovernment and eCitizenship.

1.2 Overview

While the legal aspects of downstream liability has been discussed, argued, and postulated by legal theorist since first being applied to the telecommunications industry in AT&T v. Jiffy Lube International[1]. The computer and technology sector has been watching with great interest, to the recent moves by governments, regulatory bodies, and professional associations in their efforts to establish minimal information security standards. The global attempt, while needed and long overdue, will mean that organizations with Internet connections may be liable for damages occurring as a result of cyber “attacks” that originate from their premises. The difficulty and concern with applying the doctrine of downstream liability to the computer industry, is that no system, regardless of the precautions, barriers, and defences deployed, short of unplugging and encasing in concrete, will ever be considered 100% secure. Most organizations however are aware of these risks and have allocated the resources to acquire the technical expertise needed to reduce their liability risks of being connected to the Internet. Home users however, are a different story.

2.0 Legal Background

2.1 The Disclaimer

While the author has researched the theory of downstream liability and has gotten insightful and valuable contributions from a number of experienced lawyers, please keep in mind that the author is not an attorney, nor does he claim to play one on TV. The information presented in this report, should not be considered in any way, legal advice. For legal advice, the reader is strongly encouraged to seek the services of a qualified and experienced attorney.

2.2 Legal Theory

The doctrine of downstream liability has its roots in the legal theory of negligence. While downstream liability is normally associated with information security, the Internet, and the technology / telecommunications sector, it is also relevant in other industries. Negligence, which is the most commonly utilized cause of action in tort litigations[2], refers to a party's failure to exercise a standard of reasonable care as practiced by a reasonable person under similar circumstances. The Honourable Sir Edward Hall Alderson, Baron of the Exchequer (Baron Alderson), in Blyth v Birmingham Waterworks (1856) [3] said:

> "Negligence is the omission to do something, which a reasonable man, guided upon those considerations, which ordinarily regulate the conduct of human affairs, would do, or doing something, which a prudent and reasonable man would not do. The standard demanded is thus not of perfection but of reasonableness. It is an objective standard taking no account of the defendant's incompetence - he may do the best he can and still be found negligent"

2.3 Components of Negligence

According to the document "Downstream Liability for Attack Relay and Amplification"[4] the legal term 'Negligence' can be thought of as being composed of four parts: *duty, breach, causation, and damages*. By thinking of negligence as being composed of four parts, it is easier to examine many legal theories and doctrines that may influence a tort action. In using this standard, it must be proven that the negligent party (person or company), knowing the potential risks, did not act, or failed to take the necessary steps needed in order to mitigate the risks to others.

Duty (of Care)

In order to establish negligence however the litigator must prove that the defendant had a duty of care. In the case Alexandrou v Oxford (1993) CA [5], the court found that there was no "special relationship" between the police and any particular business, in the absence of an assumption by the particular business owner, it was held by the court that there is no duty of care owed by the police to the general public. If there is no duty of care, there cannot be negligence. Proving that a defendant was careless in his work is not enough to prove negligence. Lord Macmillan said in Donohue v Stevenson (1932)[6]:

> *"The law takes no cognizance of carelessness in the abstract. It concerns itself with carelessness only where there is a duty to take care and where failure in that duty has caused damage. In such circumstances carelessness assumes the legal quality of negligence and entails the consequences in law of negligence."*

Breach (of the Duty of Care)

The terms "negligence" and "breach" are often used interchangeably in the court of law. A breach is described as the failure to uphold the responsibility of the duty of care. Depending on the case, there are a number of tests that can be used to establish if a breach has occurred. The starting point for any judge or juror in determining a breach is the 'reasonable man' or 'man on the street' test. Like the definition of negligence given by Baron Alderson in Blyth v Birmingham Waterworks, the 'reasonable man' test is a subjective test that is based on what a normal man that is free of any preconceptions or apprehensions would do in the same situation.

Another test often used is the 'expert' test. The 'expert' test is a modern interpretation of the 'reasonable man' test. It takes into account the fact that the defendant may be a company with established industry or legislative standards and best practices. In this test, the subjective nature of 'reasonable man' test is replaced with defined and irrefutable standards[7]. Using such standards as bases of determining breach of the duty of care by companies or even professionals (doctors and lawyers) is much easier.

Causation

In order to meet the requirements for negligence, the harm or damage incurred by the litigator must be a result (directly or indirectly) of a breach of the care of duty. In other words the must be a direct correlation between the harm and the breach.

Damages

Damages can be described as compensation for harm caused. There are a number of different category types that can be used in awarding compensation for negligence. While not exhaustive, the list below includes the most common:

- Compensatory Damages
- General Damages
- Special Damages
- Consequential Damages
- Future Damages
- Incidental Damages
- Punitive Damages
- Nominal Damages
- Compensatory Damages

3.0 Downstream Liability

3.1 What is Downstream Liability?

The word “Downstream” in the term *downstream liability* refers to the fact that the source of harm (attack) in the eyes of the recipient, is originating from a source (system) that is “upstream”. In other words, if Company “A” is compromised and its systems are used to attack Company “B”, Company “B” can be viewed as being downstream from Company “A”. While the applicability of downstream liability has not as yet been reviewed in the courts in any meaningful way, legal experts consider the following examples the best cases for testing its admissibility:

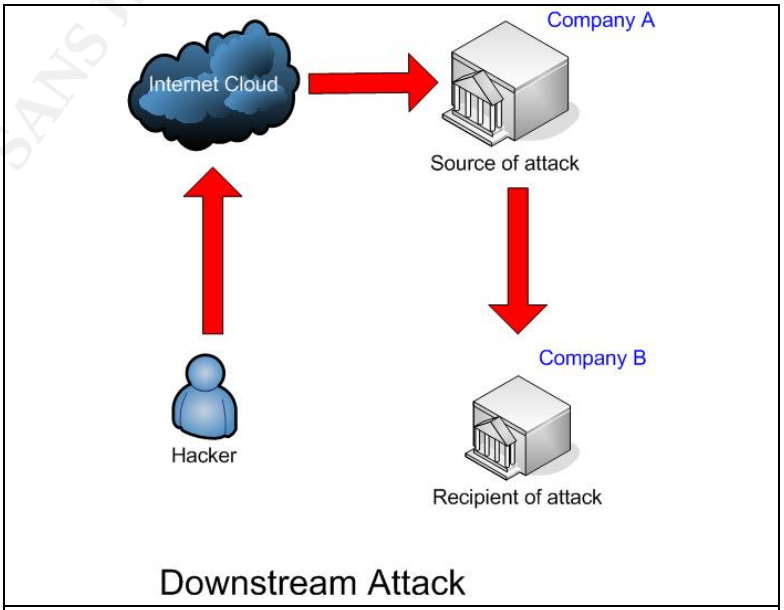

Figure 3a

- *Negligent or improper use of honey-pot systems*.
  While honey-pots[8] are mostly used as a research tool to track and record the techniques of hackers, they are also being used as a security early warning device. Honey-pots are systems that are designed to "attract" hackers (like bees to honey) by intentionally making the system vulnerable. While a honey pot in the right hands can be a valuable security tool, if not configured properly, it can also be used as a staging platform for downstream attacks.

- *Unwittingly distributing virus infected files.*
  If virus infected files are accidentally emailed to others because of a malware infection. The owner of the system sending the infected emails may be liable for damages if no precautions were taken to prevent the infection in the first place.

- *Allowing the installation of zombie software.*
  There have been many documented cases in which unprotected or unpatched systems have been compromised and used in a Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attack. If it can be proven that the owner of the system did not take basic security measures in securing the system, the owner maybe liable[9].

- *Allow the forwarding of slanderous or sexually explicit messages.*
  If a privately owned email system is used to forward or propagate messages that are intended to harm or slander the reputation or good name of a person. The owner of the email system forwarding the offending message may be liable.

- *Not installing operating system and application security patches.*
  The owner of a system may be liable for not installing well-known or critical security patches. While failure a to install operating system or application patches has not been successfully tested in the courts, costly worm infections like slammer and code red may change the status quo.

- *Unwittingly allow the distribution of sensitive private customer information.*
  While individual states like California and the Federal government have passed acts to prevent such cyber crimes, the acts could also lead to civil law suits. A Number of countries have also instituted "Safe Harbour" acts to prevent the theft or selling of personal information.

3.2 Admissibility of Downstream Liability

While the basic premise of downstream liability is based on the sound legal doctrine of tort theory, the problem with using tort law in proving liability is proving that a breach of duty did occur. In order to prove liability, there must be

negligence, in order to prove negligence; there must be an expectation of duty. If there is no expectation of duty, there cannot be liability. Is there an expectation of the care of duty to companies using information technology? In traditional tort law, the establishment of due care can be satisfied through:

- Legislation
- *Service Level Agreements*
- *Regulatory Bodies*
- *Industry Associations*
- *Internal Policies and Procedures*

In the absence of the criteria outlined above, can duty of care exist? The standard for establishing care of duty and negligence depends. While traditional tests of negligence are used routinely in establishing duty of care. Certain national and international cases have suggested that the criteria for proving care of duty could be expanded.

3.3 The Hand Test

Some legal theorist have argued that the cost of implementing effective information security measures are so low when compared to the cost to the community if no security measures are taken, that companies have an obligation and duty to protect their systems. As illustrated in *United States v. Carroll Towing Co*[10], Judge Learned Hand introduced the B < PL test. According to the Hand test, an obligation to the duty of care can be applied if the precautionary measures needed to prevent harm (B) are less than the probability of harm (P) multiplied by the monitory loss of harm (L). If the potential risks to the community are less than the cost of securing the system, then there is an automatic or implicit duty of care.

3.4 The Landlord Rule

The uncanny similarity between computerized data services and its clients and the responsibilities that landlords have to its tenants, have suggested that the similar rules of duty can also be applied to information technology. In Kline v 1500 Massachusetts Avenue Apartment Corp[11], the court declared that landlords had a duty to take “reasonable” steps to protect tenants from “foreseeable criminal acts”. The court also stated:

"[I]n the fight against crime the police are not expected to do it all; every segment of society has obligation to aid in law enforcement and minimize the opportunities for crime."[12]

Supporters of the "Landlord Rule" contend that like a landlord, business owners are in the best position to prevent its facilities (computer systems) from being used in any criminal activity.

3.5 Contributory Negligence

The doctrine of contributory negligence can also play a role in determining if a party is liable. Contributory negligence deals with situations in which the victim (recipient of an attack) "contributed" to its own attack by breaching its own obligation of the care of duty. Although the attack may have been initiated "downstream" from a source that was negligent in its duty to secure its systems, the recipient of the attack cannot claim downstream liability because its own systems were proven through the prudent man test or established information security standards to not be secure. In other words, the recipient of the downstream attack "contributed" to its own attack, and therefore showed "contributory negligence".

3.6 Economic Loss Doctrine

The uncertainty of applying liability to downstream negligence can also be shown in the doctrine of Economic Loss. The doctrine of economic loss is designed to prevent a plaintiff from suing for economic losses without evidence of physical damages[13]. In other words unless actual physical damage is proven, there is no way that the courts could apply a value to the loss. If no value can be applied, there can be no settlement. Since most information security breaches (hacker attacks), will usually only result in economic loss and not in physical damage to the organization's facilities, there is a danger that the economic loss rule (ELR) could be applied. The courts have however narrowed the applicability of the economic loss rule. In case People Express Airline v Consolidated Rail Corp., the New Jersey Supreme Court said:

"*A defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic loss that are proximately caused by its breach of duty.*

We hold therefore that a defendant owes a duty of care to take reasonable measures to avoid the risk of causing economic damages, aside from physical injury, to particular … plaintiffs comprising an identifiable class with respect to whom defendant knows or has reason to know are likely to suffer such damages from its conduct" [14].

If this ruling is applied to information technology, then the identifiable victims of a hacker attack or system breach can claim negligence and a breach of the duty of care, if the company that was breached could have foreseen the possibility of an attack and did not take adequate measures to mitigate the risks of an attack. Even if the risks were low, companies are obligated to ensure the proper information security measures are in place.

4.0 Viability of Industry and Legislative Standards

4.1 Recognised Standards

Unlike other industries or professions, where there are defined and internationally recognised minimal standards of conduct and diligence such as the International Maritime Organization (IMO)[15] and the Organization for Economic Co-operation and Development (OECD)[16], information security is inundated with standards and best practices that are similar but different. When attempting to establish a case of downstream liability, which security standard from what territory and/or industry should be used? Will one standard like HIPPA[17] be recognized as meeting the minimal standard of due care of another country or industry?

4.2 Hypothetical Example

What if Bank ABC (in The Bahamas), has its systems compromised. The systems of Bank ABC are then used to launch an attack against Bank XYZ (in Singapore). The hackers were able to successfully download confidential client information from Bank XYZ's servers to hidden directories on Bank ABC's servers. Although its systems were compromised, Bank ABC did meet minimal regulatory banking security standards of The Bahamas. The minimal security standard of the Bahamas was however, below the security standard established by the Singaporean Government. Can Bank XZY sue Bank ABC for negligence?

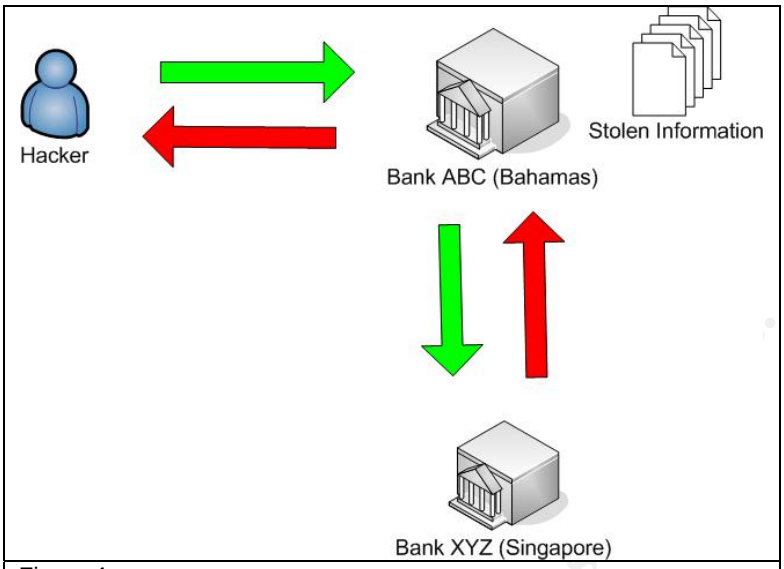

Figure 4a

4.3 Territorial Scope

Although the crime was initiated from outside the physical jurisdiction of Singapore, the country's computer misuse act includes a provision dealing with "territorial scope"[18]. As stated in section 11 of their computer misuse act:

"Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore."

The Bahamas[19] like Singapore[20] and many other jurisdictions also include provisions governing the territorial scope of the act. Clause 11 of Part III of the Bahamas computer misuse act also states (almost word for word to the Singaporean Act):

"Where an offence under this Act is committed by any person in any place outside The Bahamas, he may be dealt with as if the offence had been committed within The Bahamas."

Would Bank XYZ have a legitimate case for suing Bank ABC for Downstream Liability? It depends. Although Singapore included a "territorial scope" clause in its legislation, the clause is for all intensive purposes, unenforceable without the permission of the Bahamian courts[21] [22] . As long as Bank ABC or its subsidiaries does not have a physical, legal, or financial presence in Singapore or any country in which Singapore may have applicable mutual legal assistance treaties, Bank XYZ has no recourse if the case is tried in the jurisdiction of Singapore.

Bank XYZ if it wanted could still sue Bank ABC in Singapore. Any judgement however, would be unenforceable it would simply be a paper trial. Bank XYZ could sue Bank ABC in the courts of the Bahamas. Given the fact however, that the government of the Bahamas, through legislation, had already established minimal banking security standards, proving negligence on the part of Bank ABC would be difficult. Why would the Computer Misuse Acts (CMAs) of The Bahamas, Singapore, and numerous other countries, which are based on the British Computer Misuse Act of 1990, include a territorial clause if the clause could be deemed unenforceable in other jurisdictions? While such clauses are not implicitly enforceable, including it gives a territory the legal precedent to request help through mutual legal assistance.

4.4 Judicial Standards

Does the establishment of an industry standard exclude the applicability of subjective tests such as the “reasonable man” or the possible use of case laws? The applicability of any test or case law in establishing negligence depends on the standard used by the local court or jurisdiction. If the jurisdiction in question does not have a legislated standard, the courts, through its own fruition, could use an internationally recognized standard as part of its test. The courts however, are not obligated to use any internationally established standard without it first being passed into law. While territorial jurisdictional issues and specific tort requirements have made the likelihood of successfully winning a cross border negligence suit based on downstream liability unlikely, a downstream liability suit that is domestic in nature is still a very real possibility. With more countries legislating domestic and industry specific minimum information security standards, the burden of proving the responsibility of duty of care for companies and individuals would be easer to establish.

5.0 Liability of Home Users

5.1 Home User’s Duty of Care

If duty of care can be established or implied through legislation, and companies are compelled to conduct “reasonable” standards for the protection of their systems from attack, what would prevent a company or an individual from suing a home user for downstream negligence?

5.2 Implied Due Care

According to Mr. Calvin Seymour, an attorney for Thomas Evans and Co. (Bahamas), the establishment of a legislated minimal information security standard could open the door for negligence and liability suits against end users. He hastened to add however, that such an act would probably need to be drafted in a scope and structure similar to the road acts found in most countries. According to most road acts, individuals are required to possess a valid license before driving a vehicle on public roads. Licenses are required as a way of ensuring that drivers are aware of their duty of care when operating vehicles. If not operated properly, vehicles can be dangerous. If a driver is unfortunate enough to be involved in a traffic accident, the driver cannot claim ignorance. Having a licence ensures that the driver is aware of the rules of the road.

With the increased incidences of home based systems being used as zombies and spam-bots by criminal elements, why can't the concept of an Internet licence be applied to home users with broadband Internet access? While acts such as the Sarbanes-Oxley[23] and The Health Insurance Portability and Accountability Act (HIPPA) of the United States contain clauses that attempt to address the issue of corporate information security governance, the acts however are industry specific and cannot be used to ensure duty of care to broadband home users.

5.3 Internet Drivers License

In 1997, the European Commission created the European Computer Driving Licence Foundation (ECDL-F)[24]. The concept of a "Computer Drivers License" was pioneered by Finland in 1994 and was eventually adopted by the European community in the late 1990's. The International Computing Drivers Licence program (ICDL) is the international program modeled after the European Computer Driving Licence (ECDL). Over four million participants support the ICDL program in approximately 137 countries. The idea of a Computer Drivers Licence is central to the idea of mitigating the potential security risks posed by unprotected home and small business systems. While the present European Computer Driving Licence (ECDL) and The International Computer Driving Licence (ICDL) programs do not currently address the issue of home-user system governance, the organization is planning to introduce a new end user program called e-Citizen[25].

5.4 e-Citizenship

This new licence is geared towards users with limited exposure to using the Internet. The new e-citizen program would take about 30 hours to complete.

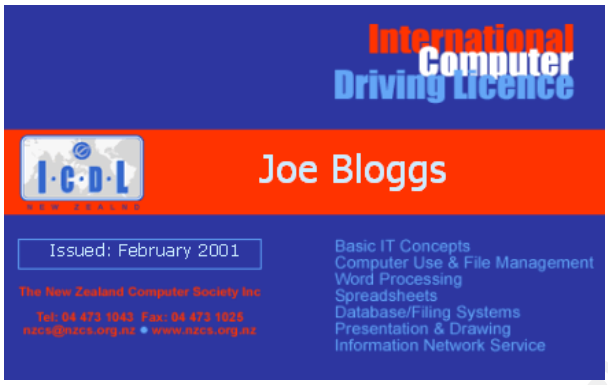

Figure 5a ICDL Driver's Licence Example

Although the proposed e-citizen outline does not introduce basic security or system governance concepts, the idea of issuing an Internet Drivers Licence based on a simple 18 to 30 hour course to teach awareness of home system governance and responsibility is intriguing. If studied and further refined, such a program would help to ensure that netizens are at least aware of their responsibilities in securing their home based systems.

6.0 Conclusion

As computer related crimes such as Denial of Service attacks, electronic break-ins, and extortion schemes continues to rise in frequency and in sophistication, international and local legal and regulatory bodies will eventually be compelled to assign more responsibility and governance toward system owners. This responsibility will first be legislated into existence by corporate governance acts such as Sarbanes-Oxley. In establishing such acts, governments are creating minimal information security standards that will be recognized by the judiciary. If the judicial systems accept the idea that duty of care is implied by the passage of corporate governance acts, the threat of downstream liability suits will increase. Although legal case studies concerning downstream liability and system negligence are currently rare, the incidences of such lawsuits will increase in frequency. While studies concerning the effect of downstream negligence have been concentrated on corporate risks, there is nothing in the legal theories or doctrines that would exclude home users from being sued for downstream liability if the proper legislation is passed.

Establishing a program similar in scope to the European Computer Driving Licence (ECDL) for home system governance is an idea that is long over due. Such a "licence" would not only reduce the amount of vulnerable systems that

maybe used as a launching platform for further attacks, but it would allow the international community to establish an internationally recognized minimal information security standards and best practices which can be followed by home users and small businesses. Governance standards such as The Health Insurance Portability and Accountability Act (HIPPA) were designed for corporations. With the majority of future system attacks most likely originating from home users and small businesses, simplified information security guide lines are needed.

---

[1] AT&T v. Jiffy Lube International, 4 CCH Computer Cases para. 46,845 (U.S. Dist. Ct. Md. 1993)

[2] Tort Law: an overview, Legal Information Institute, http://www.law.cornell.edu/topics/torts.html, (June-25-2004)

[3] Shecket, Mike; Blyth v. Birmingham Water Works Co., http://lawschool.mikeshecket.com/torts/blythvbirminghamwaterworksco.html (June-25-2004)

[4] Downstream Liability for Attack Relay and Amplification, CERT Coordination Center, http://www.cert.org/archive/pdf/Downstream_Liability.pdf (June-27-2004)

[5] Rochez, Piggot Semple; Negligence: Duty of Care, Consilio, http://www.spr-consilio.com/lawinabox/pdf/LLB_Tort_Ch05.pdf (June-21-2004)

[6] Stevenson, Donoghue; UK Law Online http://www.leeds.ac.uk/law/hamlyn/donoghue.htm (June-18-2004)

[7] Mullis & Oliphant, Tort, p 70

[8] Powell, Brad, GESS Global Security Team, Honeynet Project http://www.honeynet.org/papers/motives/forward.html (July-3-2004)

[9] Harris, Shon; DoS Defence Denying Denial-of-Service, Information Security September 2001, http://infosecuritymag.techtarget.com/articles/september01/cover.shtml#sidebar (July-4-2004)

[10] Feldman, Allen; Kim Jeonghyun, The Hand Rule And United States v. Carroll Towing Co. Reconsidered, http://www.econ.brown.edu/2002/Feldman&Kim.pdf (June-20-2004)

[11] Landlord's Duties for Criminal and Terrorist Attacks, Gross & Romanick, PC http://www.gross.com/publications/articles/art-landlord_duties.shtml (July-5-2004)

[12] Lkine v 1500 Massachusetts Avenue Apartment Corp., 439 F.2d 477, 482 (D.C. Cir. 1970);

[13] Walker, Colin; The Economic Loss Rule in Colorado, Fair And Woods, P.C. http://www.fwlaw.com/economic.html (June-18-2004)

[14] *People Express Airlines v. Consolidated Rail Corp.*, 495 A.2d. 107 (N.J. 1985)

[15] International Maritime Organization, http://www.imo.org/home.asp (June-14-2004)

[16] Organization for Economic Co-operation and Development, http://www.oecd.org/home/ (June-14-2004)

[17] Health Insurance Portability and Accountability Act of 1996, Hep-C Alert, http://www.hep-c-alert.org/links/hippa.html#hipaa (Jume-14-2004)

[18] Singapore Statutes Online, Attorney-General's Chambers, http://agcvldb4.agc.gov.sg/ (June-14-2004)

[19] The Computer Misuse Bill, 2003 (Bahamas) http://www.bahamas.gov.bs/BahamasWeb/businessandfinance.nsf/Subjects/Business+&+Finance+PDFS/$file/Computer+Misuse+Bill.pdf (June-18-2004)

[20] Scope of Jurisdictions, APEC TEL WG, http://www.apectelwg.org/apec/comple/clecb/Respons20.doc (July-10-2004)

[21] Yahoo Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 21275 (Dec. 21, 2000).

[22] Abrams, William; French Fracas—Case involving Nazi Memorabilia Rises Jurisdictional Issues, February 9, 2001; Daily Journal http://www.pillsburywinthrop.com/topics/sample.asp?id=000058130444 (July-10-2004)

[23]Sarbanes-Oxley, www.sarbanes-oxley.com (July-10-2004)

[24] Always on broadband will drive demand for consumer internet security, NetStatistica P.2, http://www.netstatistica.com/pdfs/netstatistica_security_102001.pdf (July-10-2004)

[25] European Computer Driving Licence Foundation, http://www.ecdl.com (July-11-2004)