Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Requirements For Record Keeping and Document Destruction in a Digital World

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn
More

REQUIREMENTS FOR RECORD KEEPING AND DOCUMENT DESTRUCTION IN A DIGITAL WORLD

Craig S Wright

DTh MMIT MNSA G7799 GCFA CCE
CISSP ISSAP ISSMP CISA CISM AFAIM
LLM (Candidate)

GIAC Systems and Network Auditor (GSEC)

SANS Security Essentials, SEC-401

Adviser: James Purcell

SANS

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Index

I. Abstract 5

II. Document Conventions 6

III. Executive Summary 7

Tips for effective document management 8

Introduction to document management policy 9

Applications to Internal Audit 11

Minimum Document Retention Guidelines 12

US Trends 13

Gramm-Leach-Bliley 13

The Health Insurance Portability Accountability Act 13

The Sarbanes-Oxley Act 14

Destruction of adverse documents 14

The litigation process of discovery 15

Expectation of Privacy 15

Acceptable Use Policies 15

Due Care and Due Diligence 17

The Law and Digital Forensics 18

Civil and Criminal 18

Contracts 20

Crime (Cybercrime) 20

Jurisdiction 22

Defamation and injurious falsehood 22

Harassment and Cyber Stalking 24

Pornography and obscenity 25

Privacy 25

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Searches (and the 4th Amendment) 27
Warrants 28
Anton Pillar (Civil Search) 29
Authorization 29
License 29
Intellectual property 30
Evidence Law 30
Issues that may impact and result in e-Discovery 33
Corporate Espionage 33
What is Corporate Espionage? 33
TITLE 18, PART I, CHAPTER 90, § 1831. Economic Espionage 33
§ 1832. Theft of trade secrets 34
The motives behind Corporate Espionage 35
Information to protect 35
Investigating Trademark and Copyright Infringement 37
What is a "Trademark" 37
Service Mark 37
Collective Mark 37
Certification Mark 38
Service Mark and Trade Dress 38
Trademark Eligibility and the Benefits of Registering 38
Trademark Infringement 39
TITLE 15 > CHAPTER 22 > SUBCHAPTER III > § 1125 43
Copyright Violations 50
Investigating Copyright Status 50
How Long Does a Copyright Last? 51

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The doctrine of "Fair Use" 52
Copyright Violations 53
How Copyright is Enforced? 54
Patents and Patent Infringement 56
Patent Infringement 58
US Laws related to Trademark, Patient and Copyright 60
Bibliography 79
Cases 79
Statues and Regulations 79
Standards and Other Guidelines 81
Standards 81
Other Guidelines 81
Accessibility Guidelines 81
Guidelines for Long Term Preservation 82

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

I. Abstract

In the day-to-day management of their organisation, company directors, accountants and management often overlook the importance of the documents used by the business. It is crucial to remember that the final accounts are not the only documents with a retention requirement. Further, as businesses move towards a "paperless office", they have to consider the evidentiary requirements.

In this paper, we look at document retention, legal issues such as contractual obligations, trademark and patient laws and how these are addressed.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

II. Document Conventions

When you read this practical assignment, you will see the representation of certain words in different fonts and typefaces. The representation of these types of words in this manner includes the following:

command	The representation of operating system commands uses this font style. This style indicates a command entered at a command prompt or shell.
`filename`	The representation of filenames, paths, and directory names use this style.
`computer output`	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

III. Executive Summary

Nearly all organisations generate volumes of both paper and electronic information with the dependence on electronically accumulated documents, emails mounting. The requirement to put into practice and administer an effectual document retention system is becoming more critical.

The contributing factors that act to decide on the structure of an organisation's document retention system include managing ICT spending, minimising risk (and an associated exposure), the ability to readily access data, reliability of storage and the integrity of the data, and the maintenance of a satisfactory back-up capability.

Supplementary to the commercial considerations is the legislative framework necessitating that selected documents be retained for particular minimum periods. It is a legal requirement for an organisation as a "positive legislative obligation" and as a component of good and effective corporate governance to ensure that documents are reserved correctly and destroyed when required.

An effectual document retention structure aid in compliance and reduce the risks of:

- Statutory fines and penalties (some being criminal in nature);
- Legal action and a risk of forced settlement resulting because of the cost of compliance with e-discovery requests for old emails or other documents;
- Lost cases resulting from absent email and other business records (see *Residential Funding Corp. v. DeGeorge Fin. Corp*. 306 F.3d 99 US); and
- Business losses from an insufficient archiving and recovery process.

This paper delineates many of the assorted electronic document retention requirements that possibly will apply to an organisation and presents some guidelines towards compliance.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Tips for effective document management

Chua, Wai & Toorn (2005) summaries the steps needed to implement a retention process. This paper will discuss these and other issues.

1. *Make document management part of strategic risk management*
2. *Don't just manage documents; manage the machine and people networks in which documents travel*
3. *Set up a clear document creation, retention and destruction policy*
4. *Use this policy to constantly review and update your organisation's hardware and associated software*
5. *Integrate this policy with other systems and processes that support your organisation's values and business operations*
6. *Train and regularly update your employees in active risk management*
7. *Set up a litigation document management plan*
8. *Do not destroy documents at the first sign of an investigation by regulatory agencies or of litigation*

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Introduction to document management policy

In the day-to-day management of their organisation, company directors, accountants and management often overlook the importance of the documents used by the business. It is crucial to remember that the final accounts are not the only documents with a retention requirement. Further, as businesses move towards a "paperless office", they have to consider the evidentiary requirements.

It is usually when things go wrong that current documents are of the greatest significance. For instance, the source documents are the ones that auditors will treat with special care. It there is an issue with the accounts, it is important to be able to go into the history of the transaction. Oral testimony without evidentiary support is not reliable. Documents may be used to trace records and their absence often says more than their existence, but not in a good way.

This is why companies need to take care in the management of their documents. Grave consideration should be given to the destruction of any document. That is what it should be noted that the destruction of documents in some cases maybe not just illegal but criminal. For instance, a company officer or director who destroys or falsifies a document affecting the company's property or affairs is liable to prosecution under the Australian Corporations Act 2001, sections 1308 - 1309.

It is a requirement that the person involved proves that the intention to deceive was not associated with the destruction. In many cases, these are statutory strict liability offences. In other words, the prosecution only needs to prove the facts it is up to you to disprove intent. This is not something that is easy to do in a court of law. In fact, S 1309 (2), Australian Corporations Act 2001 makes it an offence if the officer/employee fails to take reasonable steps to ensure the accuracy and protection about the records.

In Victoria, recent changes to the Crimes Act (1958) [Crimes (Document Destruction) Act 2006; Act No. 6/2006] have created "*a new offence in relation to the destruction of a document or other thing that is, or is reasonably likely to be, required as evidence in a legal proceeding*". This act, punishable by indictment for a term of up to five years imprisonment affects anyone who destroys or authorises the destruction of any document that may be used in a legal proceeding (including potential future legal proceedings).

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Under section 286(1) of the Corporations Act, a company must keep "written financial records that:

- *correctly record and explain its transactions and financial position and performance; and*
- *would make true and fair financial statements able to be prepared and audited."*

If a dispute has previously arisen or is considered likely, it is very hazardous to destroy any documents. Cases where provisions for litigation had been included in audit reports are a definite example. In instances where it is probable that a dispute may arise or after a dispute has begun, a conscious choice to destroy documents could make one liable under the criminal offence of obstructing or perverting the course of justice.

Ask any forensic accountant; omitted documents usually leave telltale indications of their existence due to being referred to in existing documents. If the case goes to court, it is necessary to list not only documents in one's possession, custody or power, but also those that once existed that have been destroyed.

The destruction of documents can adversely influence a case through interference. In the UK, *Infabrics v Jaytex* ([1982] AC 1 (HL)) demonstrates such a case. After the commencement of the case, it was discovered that most of the invoices, stock records and similar documents had been destroyed.

The judge stated that he was "*not prepared to give the defendants the benefit of any doubt or to draw an inference in their favour where a document, if not destroyed, would have established the matter beyond doubt*"

With the increasing prevalence of electronic documents, companies need to ensure and updated their document retention policies. These policies should not be disorganized or ad hoc. Once we could look to limitations, for how long we should keep files, most professions keeping papers for at least seven years. Recent decisions of the court and the requirement to keep records for a period after the final transaction make this more difficult (not seven years from when the document was created!).

Always remember "It sensible that a company adopt a document retention policy to ensure that documents are only discarded or destroyed in accordance with the law and in a systematic manner" (Phillip, 2006).

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

With the readily available advanced technology that is available, it is prudent to preserve files using scanners and other electronic storage means rather than destroy them. A written policy on document destruction and retention, to be applied consistently, is a shrewd move.

Applications to Internal Audit

Document management is not an issue confined to Australia and the UK. Rather it is an ever-growing concern for organisations throughout the world. In particular, the increasing use and complexity of document management systems and databases is driving an invigorated need to instigate effective controls.

It is no longer enough for the internal IT auditor to rely on an isolated snapshot of the system. It is essential that an understanding of document retention requirements based on the jurisdictional idiosyncrasies be maintained.

There are a number of steps that the internal auditor can use to aid in auditing electronic documents. By incorporating controls into databases and other systems, the audit staff are able to ensure that the legislative requirements are being met. Some steps that may be undertaken include:

1. Classifying all documents that are scanned or electronically created using systems of automated controls and allocations,
2. using digital analysis techniques and data mining to search through system storage and data warehouses for keywords and classifications,
3. configuring key fields in databases and making rules to create isolated copies of required documents,
4. formal policies and procedures,
5. network scanning for defined a classifications.

Of particular note, it is essential to remember that e-mail is an internal document and may as such be covered by the record-keeping requirements. It seems to be generally unknown that e-mails concerning product defects are likely to be required to be held under the product liability constraints for up to 10 years from being sent.

So next time your organisation decides to purge files, e-mails and other miscellaneous electronic documents have a thought for the possible repercussions before you do so. There is more to document retention than managing disk space.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Minimum Document Retention Guidelines

	Australia/NZ	USA	UK
Basic Commercial Contracts	6 years after discharge or completion	4 years after discharge or completion	6 years after discharge or completion
Deeds	12 years after discharge	A minimum of 6 years after discharge	12 years after discharge
Land contracts	12 years after discharge	6 years after discharge	12 years after discharge
Product liability	A minimum of 7 years	Permanent	A minimum of 10 years
Patent deeds	20 years	25 years	20 years
Trade marks	Life of trade mark plus 6 years	Life of trade mark plus 25 years	Life of trade mark plus 6 years
Copyright	75 years after author's death	120 years after author's death	50 years after author's death
Contracts and agreements (government construction, partnership, employment, labour, etc.)	A minimum of 6 years	Permanent	A minimum of 7 years
Capital stock and bond records	7 years after discharge	Permanent	12 years after discharge

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

US Trends

Regulatory trends in the US are often indicative of future trends in other countries. However, US laws may also be immediately relevant to subsidiaries of US Securities Exchange Commission (SEC) entities and for any Australian organisations to which a US SEC entity outsources it's document management and information systems.

Gramm-Leach-Bliley

The Financial Modernization Act of 1999, or the Gramm-Leach-Bliley Act (GLB), defines stringent requirements for businesses to protect all personal information that is collected. The GLB has two requirements that direct the collection and use of private financial information. These are the:

a. Financial Privacy Rule, and

b. Safeguards Rule.

The Financial Privacy Rule affects all financial institutions. These are roughly defined to include mortgage brokers, tax preparers, and possibly merchants. Financial institutions must present clients with regular privacy notices elucidating the information that is collected about its clientele and how that information is utilised, distributed, and protected. Clients have the right to "opt out" which in effect means that their information can not be shared. On a privacy policy changes, clients are required to be notified and offered another opportunity to opt out.

The US Attorney General enforces Gramm-Leach-Bliley. It has provisos for fines of up to $100,000 to the financial institution for each violation and civil penalties of up to $10,000 for the officers and directors of an organisation.

The Health Insurance Portability Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA or the Kennedy-Kassebaum Act) was implemented as law in 1996. The sections relevant to security and this paper are:

- The Privacy Rule, and
- The Security Rule.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The Privacy Rule defines patient medical records or protected healthcare information (PHI) and controls the use and disclosure of PHI, necessitating well-built measures to certify patient privacy.

The Security Rule balances the Privacy rule by defining administrative, physical, and technical security safeguards required to protect PHI. Security standards are defined for each of these groupings. HIPAA provides rigid sentences for those who violate it, including criminal prosecution.

The Sarbanes-Oxley Act

The Sarbanes-Oxley Act (or "The Public Company Accounting Reform and Investor Protection Act of 2002") is typically called SOX or Sarbanes-Oxley. SOX was intended to offset a perceived decline in public trust after a series of accounting outrages. SOX establishes enhanced accounting and auditing standards for all publicly traded companies in the US and the affiliates of these companies. It mandates the evaluation and disclosure of the effectiveness of the internal controls implemented by a company. The chief executive officer and chief financial officer of the company are required to certify financial reports.

SOX requires company executives to be accountable for the security, accuracy, and reliability of all IT systems used in reporting financial information. This accountability must be reflected in the internal controls used to manage the companies' information systems used for the processes of financial reporting.

Destruction of adverse documents

It is an offence to destroy any document that is or may be used as evidence in an ongoing or potential judicial proceeding in most western (at least the common law) jurisdictions. An organisation must not destroy documents on the foundation that the evidence unfavourable. The penalties for the destruction of documents that are suspected to **possibly** be subject to litigation may perhaps end in a charge of obstruction to justice.

Adverse inferences are often upheld in litigation if a party cannot produce the required documents. There is also the hazard of reputation damage. In *British American Tobacco Australia Services Limited v Roxanne Joy Cowell* for the estate of *Rolah Ann McCabe [2002] VSCA 197* the Judge in first instance seriously denounced

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

BAT for the methodical destruction of a large number of records. Documents that may retain as evidence value need to be retained. Sardonically implementing a record retention policy without taking proper precautions will generally draw an adverse inference from the court if there is any departure from the policy.

The consequence is that policy also necessitates ongoing education about the policy and the procedures utilised to enforce it and constant re-examination of its content.

The litigation process of discovery

Discovery is the progression of events that follow the initiation of legal proceedings. A matter will proceed to Court only after all parties have delivered up relevant documents or have presented testimony that they can not provide these documents. The process of e-discovery involves electronic records such as emails.

Rigidly enforced periods make it vital for the parties to be able to retrieve documents and emails promptly.

Expectation of Privacy

Privacy in the workplace is a contentious subject. The definitions of privacy, and its means of protection, vary by jurisdiction. Employee email is commonplace and is used for both work and private means.

Organisations have stringent legal requirements in the European Union, Australia, the United States, and other jurisdictions to guard information on private individuals from unauthorised disclosure.

Acceptable Use Policies

Enlightening workers of acceptable behaviour protects an organisation from liability, encourages compliance, and is a requirement if disciplinary action is to be enforceable.

As a minimum document retention policy is required to address the following areas:

1. Human resource
2. Administration

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

3. Accounting and finance
4. Legal (including contracts)
5. Drawings and specifications
6. Studies and reports
7. Calculations and designs (including Patient and Trade/Service Marks)
8. Construction
9. Approvals and reviews
10. Correspondence

According to the NSoPE (2005), any document retention policy should include:

1. *Any document retention policy that is created should be followed consistently for every project. If deviation from the formal policy is made for a particular project, the firm should document why the deviation was made. If retention policies differ for different projects, that should also be included in the written policy.*
2. *If a policy is created that allows for destruction of documents, ensure that the document destruction is absolute and document the date of destruction.*
3. *Make sure that document retention polices are written, especially if the policy includes document destruction that otherwise might seem suspicious.*
4. *Ensure that individuals in charge of document retention or destruction are trustworthy, especially for confidential items, such as items related to lawsuits, payroll, or competitive information.*
5. *Ensure that stored documents are organized, labelled, secure, and easy to retrieve.*
6. *Do not destroy documentation after notice of a lawsuit has been served, regardless of the written policy related to those documents.*

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Due Care and Due Diligence

Management is required to implement and preserve a suitable set of internal controls to check illegal and unscrupulous goings-on. A failure to implement due care and due diligence can constitute negligence.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The Law and Digital Forensics

The foremost dilemma with the study of the electronic law is that it is very complicated to confine its study within simple parameters. Internet and E-commerce do not define a distinct area of law as with contract and tort law. Electronic law crosses many legal disciplines, each of which can be studied individually. Examples of a range of areas of law that electronic, e-commerce and Internet law touch upon can be seen below.

In fact, the majority of cyber crimes are already addressed by existing laws. In most cases, cyber crimes are just age-old crimes committed using a new technology. Identity theft for instance has existed for hundreds of years, only now the speed and volume and hence the effect of the crime has increased.

New challenges do arise through the nature of widely distributed networks such as the Internet. Some legal jurisdictions have addressed this issue through the mending of existing laws. Most however, have adopted an approach where they define solutions to a perceived unique legal problem through the creation of separate digital laws. In particular, these are manifest in the numerous additions to computer crime statutes in their criminal codes.

Of particular confusion to many people is the distinction between what is illegal in what is criminal. This however is not a distinction solely confined to electronic law. It is important to note that although many actions are illegal they may not be criminal in nature. This is important as the evidentiary requirements in criminal cases are far stricter than in civil litigation. It needs to be noted the level of professionalism and standards attached to handling evidence should be maintained equally in either civil war criminal cases.

This section will endeavor to summarize the primary areas of electronic law that the forensic practitioner is likely to encounter.

Civil and Criminal

One of the key distinctions between all legal cases concerned is the distinction between what is criminal and civil in a legal nature. Generally, a criminal case consists of one where the state is punishing a person due to their undesired behavior. A civil case revolves around a person or company bringing action to recover damages

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

or stop some behaviour (e.g. through injunction). The forensic practitioner is likely to encounter either type of case dependent on whom they work for.

Criminal or penal law concerns those issues that are believed to affect the whole of the population. The fundamentals of criminal law are known as the *actus reus* (or the guilty act) and the *mens rea* (the guilty mind) of the crime. The *actus reus* covers the actual act of having committed the crime. This is the physical element. In hacking, the physical act could be sitting at the offender's computer and starting an attack script.

The *mens rea* of an act is the mental element associated with the deed. This is more commonly known as intent. In some instances recklessness may suffice to cover the element of intent. An example of intent could come from something like bragging. A hacker who announces over IRC the intent to break into a site could be said to have intent. Conversely, a penetration tester who unknowingly attacks on sites belonging to someone else under the honest belief that the site belonged to their client would either be at worst reckless if they had not checked the address or could be shown to not have intent if they are acting in good faith.

There are a variety of civil actions. Primarily these are either contract or tort actions.

A contract is any agreement where there is offer, acceptance and consideration. Consideration may be of monetary nature or anything else of value. Torts are civil wrongs, which involve violations of the personal, business or property interests of persons whom a reasonable person ought to have foreseen would be impacted by their actions, if they were not prudently carried out.

As an example of a tort, if you allow Bob to run his website on your server but do not give him any permission to do anything else and then he subsequently uses the server to send large volumes of unsolicited e-mail having your site blacklisted, you could recover damages. The rule is, if you let somebody use your property, and they use it in a way you did not anticipate or give authorization (license) for, you may recover for this *tort of conversion*. On the other hand, if you had offered the site to Bob for a monthly fee which he accepted, the action would be for breach of contract.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

At times there will be occasions where the forensics professional will be involved gathering information that is not strictly attached to a legal action. Some examples include cases where the material is:

- Highly offensive but not unlawful
- Breach of procedure, policy etc
- Inappropriate only

In "at will" employment situations, no legal wrong may have been committed. However, an employer may seek to minimize risk by removing the party who is the source of at risk.

Contracts

A simple definition of e-commerce is the creation of a contract electronically. It should come as a modest revelation that the law of contract is relevant to the study of e-commerce and hence will relate to the forensic analysis of computers. Questions can be posed of contract law, for instance, do the common principles of contract formation concern transactions over the Internet? Conversely, do problems arise because of this new media?

The forensic practitioner may be called in to determine the origins and scope of contractual dealing. In particular, e-mail conversations and saved copies of contracts and associated documents may often be recovered.

Crime (Cybercrime)

There will always be those in the world who wish to gain some benefit without actually paying for it. As a result the electronic law will also cross over certain aspects of criminal law. Whether by an outsider or through the actions of disloyal employees, crime is something that is likely to remain with us for the foreseeable future. The Internet and digital networks create new vulnerabilities and methods that criminals can exploit for their own gain.

Most of the existing crimes can be replicated and transacted with the aid of an online environment. Further, novel new crimes designed to exploit the features and advantages of the Internet and other digital networks have emerged and are likely to continue to emerge in the future. Some example criminal activities that have benefited from the advances in digital technology include:

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Computer break-ins (or Trespass) including the illegal access to the whole or any part of a computer system without right;
- Illegal interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system;
- Data Interference or the damaging, deletion, deterioration, alteration or suppression of computer data without authorization;
- Interfering with a system or the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;
- Possession of obscenity/prohibited pornography (e.g. child pornography and bestiality);
- Industrial espionage;
- E-mail Fraud;
- Harassment;
- Web page defacements (cyber vandalism);
- Theft of company documents.

While none of these crimes is wholly new, the ease in which they may be committed and the difficulty in capturing the offender has added a new dimension to crime. For instance, it is unlikely that law enforcement officials will be able to take action against many cyber-criminals unless the majority of countries first enact laws that criminalize the behaviour of the offenders.

Some of the primary issues that face law enforcement in cybercrime cases include:

- Increased Investigative Costs due to the need for high priced specialists;
- The difficulties of conducting “Real Time” Investigations;
- The ease of Anonymity on the Internet;
- Difficulties with Jurisdictional issues;
- The rate at which Technology is evolving; and
- The Irrelevance of geographic distance.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Jurisdiction

Jurisdiction addresses the question; "where should the case be heard?" in many places, including the US, this is further complicated through the requirement for the court have two types of jurisdiction in order to hear a case. This is the court needs both subject matter jurisdiction and personal jurisdiction.

Subject matter jurisdiction is the power of the court to hear the particular type of dispute being brought before the court. For example, criminal courts in matters concerning crimes; family Court will address matters such as divorce; and a number of civil courts will hold a variety of tortuous and contractual matters.

Personal jurisdiction is related to the power to enforce a judgment over a defendant. This is often a question that is difficult to answer. A jurisdiction will define in statute how far believes it can reasonably assert personal jurisdiction over another. In some cases this may only extend locally, in others the perceived jurisdiction may encompass the entire globe. The difficulty arises when these jurisdictional boundaries conflict.

There are a variety of fundamental challenges imposed through the borderless nature of the Internet and electronic networks. In everything from electronic commerce to cyber crime, domestic law has been fundamentally challenged. The issue of jurisdiction in electronic law concerns both the location of the parties to the matter and the location of the computers or other systems.

This matter can be complicated due to a one-party impacting a computer in another jurisdiction which is owned or controlled by separate party in the third jurisdiction. In these cases the difficulty of international law and treaty conventions becomes critical to the effect of handling of data.

Defamation and injurious falsehood

Even in the US with strictly defined protections to the rights of free speech and is trying in the Constitution, there is no overriding right of free speech. There is no doubt that you can defame someone using an electronic message. A publication of a statement about a person is by definition defamatory if it is likely to result in the loss of reputation as viewed by a reasonable person.

Generally the following must be present to establish defamation:

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

1. A defamatory statement (or material) or imputation;
2. The statement (or material) identifies the plaintiff; and
3. The statement (or material) is published to a third person, i.e. at least one person supplementary to the plaintiff.

Where an attack is made against the offerings of an organization, it may be possible to establish that there has been an injurious falsehood. In this case the organization may be able to obtain damages compensated for the damage suffered. In injurious falsehood cases and is required that the plaintiff proved that the matter was maliciously published and that damage resulted. Digital forensic methods are utilized in tracing compensations that may offer proof of malicious intent.

In defamation cases the plaintiff does not need to prove that the statement against them was false. It is up to the defendant to prove the nature of their claim.

The primary defences to defamation:

1. The imputation is true or substantially true;
2. In many jurisdictions the doctrine of absolute privilege will protect anything said in court or Parliament. This is also extended to transcripts of these proceedings as qualified privilege as long as the statements are accurately reported;
3. Where there is a requirement to divulge (for example reporting crimes to authorities);
4. Where specific jurisdictional projections or statues exist (e.g. whistleblower laws);
5. Political debate and discussion;
6. Fair comment; and
7. Consent.

Defamatory statements or material must be published to at least one person. If a single person views information that has been uploaded onto the Internet, then that information is taken to have been published. Traditionally, verbal and published imputations have been distinguished respectively as slander (in cases of verbal abuse) and libel (in cases of published materials).

The digital forensic practitioner will primarily become involved defamation in civil cases. This are may be from either the perspective of the defendant or the

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

plaintiff. An example of such involvement would include determining the source of an anonymous e-mail of the author of a comment on a webpage. Even where e-mail has been through anonymous accounts, traces may exist on an offender's computer.

Harassment and Cyber Stalking

Whether it is racial or sexual harassment, stalking, bullying at work or neighbours from hell, harassment is a form of discrimination that is generally prohibited by legislation. In the workplace is something that employers must not tolerate. Harassment is any form of unwelcome, unsolicited or unreciprocated behaviour that a reasonable person would consider offensive, humiliating or intimidating.

Harassment includes behaviour that has this effect because it is of a sexual nature or of the targets a person due to a particular characteristic (such as race, sexuality, disability, age, national origin or gender). Included in harassment obscene communications, derogatory remarks or slurs, communications (including jokes or visual images) that are designed to ridicule the mean or torment another person by focusing on a personal characteristic, and stalking (whether physically or via cyber stalking).

It is worth noting that a single incident can constitute harassment and that the harassed person did not have been disadvantaged. In fact, the intentions of the person who did the harassing are irrelevant. An employer will be liable where an employee commits an act of harassment if they cannot establish that they took reasonable steps to prevent it.

Sexual harassment is the most common form that comes before a court. There can exist female harassment of males, same-sex harassment and harassment may occur through the publication of images or statements of a sexual nature.

Cyberstalking is the distribution of malicious communication through e-mail and the internet. Although based on new technology, it is in principle precisely the same as any other form of malicious communication and can be dealt with through the usual civil and criminal law methods. The distribution of offensive e-mails through the Internet and such communication will also constitute an offence under a variety of statutes (such as the *Malicious Communications Act* in the UK).

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Pornography and obscenity

Pornography is big business on the Internet and has even been seen by some as its foundation. In the US, pornography is protected a speech under the first Amendment to the Constitution. Obscenity on the other hand is not protected. Obscenity may be legally possessed in an individual's private home, but generally its distribution is illegal. The Miller test, as articulated by the Supreme Court in the 1973 case of Miller v. California is used in the US to determine whether expression has crossed the line from being pornography to obscenity.

The test was defined in the case as:

1. *Would the average person, applying contemporary community standards, find that the work, taken as a whole, appeals to the prudent interest?*
2. *Does the work depict or describe, in a patently offensive way, sexual conduct specifically defined by applicable state law?*
3. Does the work, taken as a whole, like serious literary, artistic, political, or scientific value?

The US Congress tried to address the problem of the ease of access to this type of material by children through the Telecommunications Act of 1996. Title V of the act (commonly known as the Communications Decency Act, CDA) included provisions with the intent to regulate the dissemination on the Internet of material deemed to be inappropriate to minors. Shortly afterwards however, the Supreme Court struck down sections 223 (a) and (d) in Reno v. American Civil Liberties Union et. al. result of these and subsequent cases is that there is no clear "community standard" which defines obscenity.

In cases such as child pornography, this is being clearly held not to be expression protected by the First Amendment. The Internet has provided offenders with greater access to obscene materials and even aids in the solicitation of children by paedophiles.

Privacy

US Justice Cooley defined privacy is a right to be left alone. Others see privacy as a right to be anonymous. These different definitions imply different implications.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

In legal terms, privacy is a two headed coin. On one side there is the right to be free from government intrusion; on the other there is a right to be free from intrusions from private individuals. The nature of this right is a protection of our private lives.

The right of privacy comes from the common law. In particular there are four pillars created through tort. These are:

1. The right to stop another appropriating your name or likeness;
2. The right to be free from unreasonable intrusion through the intentional interference with another person's interests in solitude and seclusion;
3. Freedom from false light. This is freedom from publicity which presents a person to the public in a manner that damages their reputation (see defamation); and
4. And freedom from public disclosure of private facts.

In addition, governments have imposed statutes aimed at further increasing the rights to privacy. In Europe, the right to privacy has been integrated into European Treaty convention.

The primary statutes enacted in the US to protect privacy include:

- Electronic Communications Privacy Act of 2000, which was designed to regulate the interception of electronic indications such as e-mail;
- The Privacy Act of 1974. 5 U.S.C. § 552a which has imposed limits on the amount of personal information that can be collected by federal agencies;
- The Fair Credit Reporting Act (FCRA) as amended October 13, 2006 regulates the collection and use of personal data I credit reporting agencies;
- The Federal Right to Privacy Act (1978) limits the amount of information from customer files that financial institutions may disclose to the US federal government;
- The Video Privacy Protection Act of 1988 prohibits movie rental companies from disclosing customer names and addresses on the subject matter of their purchases for marketing use;
- The Cable Communications Policy Act of 1984 prohibits cable television companies from using their systems to collect personal data concerning their subscribers without their express consent;

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- The Equal Credit Opportunity Act (ECOA) prohibits creditors from collecting data from applicants including gender, race, religion, birth control practices, national origin, and similar information;
- The Family Educational Rights and Privacy Act (FERPA) of 1974 allows students to examine and challenge their educational transcripts and other records.

The word *privacy* appears at no point in the US Constitution. The result is that the right to privacy has developed as a separate body of law. In the US, the Fourth Amendment to the Constitution with its prohibition against "unreasonable searches and seizures" has built the foundation for many of these rights.

Searches (and the 4th Amendment)

In much of the common law world (including the USA, UK, Canada, NZ and Australia), law enforcement needs to obtain a legal authorization in order to search and seize evidence. Generally, this power is granted through a request for a search warrant which states the grounds for the application including the law which has been broken. In the United States and the United Kingdom the requirements further require that the application describes the specific premises to be searched as well as the items being sought.

In the US, the Fourth Amendment and the Electronic Communications Privacy Act (ECPA) determine the awfulness of a search. The Fourth Amendment only applies to government searches (such as those conducted by law enforcement officials). The ECPA applies to everyone (whether government or private) and prohibits the unlawful interception or access to electronic Communications.

In the physical world there is a real limit on the length of time during which a search can be conducted. This rule does not impose much of a limit on electronic searches. As the investigator is able to make a copy of the digital evidence (such as a hard drive), they are able to continue to search these files both for "strings" which are beyond the scope of the original warrant and also at their leisure.

Neither the fourth Amendment nor Federal rules of criminal procedure required the investigator to promptly search the evidence. In fact, US federal law provides little over the return of property seized pursuant to warrant. The suspect must file motion in court in which they either prove that this seizure was illegal or that

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

the investigator no longer has any need to retain the evidence to either have the digital evidence returned or destroyed.

As a result, law enforcement officials can keep a copy of any digital evidence they had seized under a warrant and continue to search it without any effective time limit. Fourth Amendment rules do not provide useful guidelines for investigators conduct even in Digital forensic labs. There are no limitations of the regions of a hard drive that a forensic computer analyst may examine for evidence and the analyst may continue to look for evidence of other crimes.

The fourth Amendment rule is that an investigator executing a warrant is able to look in any place listed on the warrant where evidence might conceivably be concealed. Traditionally, an investigator was precluded from looking into any location is more than the evidence they wish to seize. Electronic evidence however may be stored anywhere. The result is that an investigator can electronically look anywhere in search of digital evidence.

Katz v. United States [389 US 347, 351 (1967)] stated that "the fourth Amendment protects people, not places". The result is that the fourth Amendment continues to be deeply tied to physical places.

Warrants

To be accepted as evidence in court a warrant is generally required for law enforcement to search and seize evidence. There are exceptions for this need including:

1. When the evidence is in plain view all sight;
2. Where consent to search has been granted; and
3. Situations involving some exigency, such as emergency threatening life or physical harm.

To obtain a search warrant, an investigator needs to convince the court of the following three points:

1. Some criminal act has been committed;
2. Evidence of a crime exists and is available; and
3. It is probable that the evidence is likely to be found at the place being searched.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Anton Pillar (Civil Search)

An Anton Pillar order is a civil court order providing for the right to search premises and seize evidence without prior warning. In the US, the Business Software Alliance has used these orders as a remedy when they are attempting to stop illegal software use (termed Software Piracy) and Copyright Infringement to achieve the recovery of property.

Ormrod LJ in Anton Pillar KG v. Manufacturing Processes Limited in 1976 (UK) defined the three-step test for granting this order:

1. There is an extremely strong prima facie case against the respondent,
2. The damage, potential or actual, must be very serious for the applicant, and
3. There must be clear evidence that the respondents have in their possession incriminating documents or things and that there is a real possibility that they may destroy such material before an inter partes application is able to be in court.

In the UK, Anton Pillar orders have been (for the most part) outmoded by the introduction of a statutory Search order under the Civil Procedure Act 1997. These applications are still common in many places such as Canada and France.

Authorization

In legal terms, authorization is defined as the right to use a product or service within the agreed terms. Authorization may be implied (such as when using a public website for the purposes to which the site owner designed it) or explicit (such as occurs when using Internet banking after having authenticated using one's own valid credentials).

In legal terms, the granting of permissions through authorization is in effect the granting of a licence.

License

To license or grant license is to give permission or authorization. A license is the demonstration of that permission. In cases of software for instance, the license is the right to use the software as long as the user agrees to the terms of the license. License may be granted by a party ("licensor") to another party ("licensee") as a

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

constituent of an agreement between those parties. A simple explanation of a license is “a promise by the licensor not to sue the licensee”.

In intellectual property law a licensor grants the licensee the rights to do some action (such as install software, make use of a patented invention or even watch a movie) without fear of retribution through an intellectual property infringement.

Intellectual property

Intellectual property laws concern the protection of another’s intellectual designs and works. It is important to understand that when surfing the Internet, what is seen is protected by copyright. In addition the actual website visited the domain and host address is often the subject of trade mark or passing off litigation.

The law of Intellectual Property is aimed at the safeguarding of peoples’ ideas. Intellectual property is an expanse of law that deals with the protection of intangible items such as ideas and creativity that exist in some tangible form (such as a movie, music CD, name or design). There are many separate subject areas in Intellectual Property law, including:

- Copyright
- Confidence
- Design rights
- Domain names
- Moral rights
- Performance rights
- Patents
- Passing off
- Trade marks

Evidence Law

Electronic evidence in law is the legal recognition and evidential value in litigation of evidence in digital format. Of particular importance the US Federal Rules of Evidence, the UK Police and Criminal Evidence Act (PACE) and the UK Civil Evidence Act. Similar rules of evidence apply in other jurisdictions.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Before admitting evidence, a court will generally ensure that it is both the relevant to the case and also evaluate it to ensure that it satisfactorily fulfils what it is claimed to provide. A court needs to determine whether the evidence is hearsay and otherwise determine its admissibility.

The primary issues concerning digital evidence are associated with the ease to which documents may be copied or altered and the resultant effect on its value as evidence in court as well as the impact on civil liberties. The nature of digital technologies has compounded the amount of information that is available. As a consequence, it is far easier to violate the privacy rights and other civil rights of the individual in this digital age.

The most common mistake made in obtaining digital evidence occurs when it has been taken without authorization. Generally a warrant or court order must be granted for the collection of the evidence before it will be admissible. There are exceptions to this rule, which had been listed above in the section on warrants.

The evidence to be admissible it must go through a process known as authentication, which is designed to determine whether the evidence meets what its proponent claims and subsequently to attempt to determine its probative weight. Even in cases where reasonable doubt exists as to the reliability of electronic evidence, this may not make it inadmissible in court. It will however reduce the weight it is given by the Court.

Rules of *Best Evidence* were originally introduced to prevent a party from misrepresenting materials (such as written documents, photographs or recordings) by simply accepting the testimony regarding the contents. With digital evidence, an exact duplicate can generally be made. The result is that a copy is generally acceptable in court. In fact, statutory provisions (such as the Electronic Transactions Act, 1999 Australia) may determine that a digital copy or extraction of a physical document is equivalent to the original printed form. Further, due to the nature of embedded materials (such as macros in Microsoft Word), the digital format may even be preferable.

The distinction between correct and circumstantial evidence is that direct evidence categorically establishes the fact. Circumstantial evidence on the other hand is only suggestive of the fact. Authentication logs are generally accepted as direct evidence short of proof that another party used the access account.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The rules of *Scientific Evidence* apply to digital forensics. In the US, Daubert v. Merrell Dow Pharmaceuticals, [509 U.S. 579 (1993)] set the standard for evaluating scientific evidence. The test developed in this case consists of:

1. A determination whether the theory or technique is capable of or has been tested;
2. The existence and maintenance of standards controlling techniques of operation and whether these are likely to result in a high known or potential error rate;
3. As to whether the theory or technique has been rigorously subjected to peer review and publication; and
4. If the theory or technique is subject to "general acceptance" within the relevant scientific community.

For the most part (and even though error rates have not been established the most digital forensic tools) electronic evidence has been accepted by the courts scientific evidence. Currently, the most effective approach to validating the methodologies and approach used by an investigator remains peer review. For this reason, it remains good practice to have another investigator double check any findings using multiple tools or techniques to ensure the reliability and repeatability of the process.

"*Evidence is hearsay where a statement in court repeats a statement made out of court in order to prove the truth of the content of the out-of-court statement*." (Hoey, 1996). An example of hearsay evidence would apply where a suspect has sent an e-mail purporting to have committed a crime. Law enforcement officials would still need other evidence (such as a confession) to prove this fact.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Issues that may impact and result in e-Discovery

Corporate Espionage

In respect to Corporate Espionage and the methods used to combat it, the questions we have to ask include:

1. Why does Corporate Espionage occur?
2. Who are these 21st century techno-spies?
3. How do they go about stealing?
4. What do they really take?
5. What can we do about it?

To fully understand Corporate Espionage in the 21st Century requires an understanding of the Information Age or Age of Technology. Modern Espionage does not just concern the government and is more than spies stealing military secrets. Corporate Espionage in the new global business environment is emerging as the primary 21st century means for creating a competitive advantage – whether as a country, organization, country, business, or military power.

What is Corporate Espionage?

Corporate Espionage is defined under "theft of trade secrets" and "economic espionage" by the US Economic Espionage Act of 1996 (Title 18 UCS 1831). It is a federal criminal offence.

The Economic Espionage Act became effective as of 11th October, 1996. It was originally aimed at bringing an end to the foreign theft of U.S. information. It criminalizes on a federal level the theft of trade secrets. It has two main provisions that cover state-sponsored (1831) and commercial (1832) thefts.

TITLE 18, PART I, CHAPTER 90, § 1831. Economic Espionage

(a) In General.— Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) Organizations.— Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

§ 1832. Theft of trade secrets

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will , injure any owner of that trade secret, knowingly-

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

The motives behind Corporate Espionage

The primary motivations for Corporate Espionage include:

1. Theft of trade secrets for economic gain.
2. Attempting to monopolize a product or other offering in a selected market.
3. To acquire competitive advantage in domestic and global markets.
4. Threats of computer technology.
5. Privacy violations.

Basically, the threats are the same as they have always been; only the media has evolved to make it easier to commit the crime.

Information to protect

The corporate spy will seek anything that provides them with an advantage or profit. Some of the possible sources of Information include:

- Documents – whether completed or still in draft, and working notes or scrap paper
- Computer Based Information
- Photographs, Maps and Charts
- Internal Correspondence and email
- Legal and Regulatory Filings
- Company Intranet access and Publications
- Formal meeting minutes or transcripts
- Casual conservations
- Conversations at trade shows and events.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

A competitive organization may also be able to make use of and gain an advantage using:

- Marketing and product plans (esp. prior to release)
- Source code
- Corporate strategies and plans
- Marketing, advertising and packaging expenditures
- Pricing issues, strategies, lists
- R&D, manufacturing processes and technological operations
- Target markets and prospect information
- Plant closures and development
- Product designs, development and costs
- Staffing, operations, org charts, wage/salary
- Partner and contract arrangements (including delivery, pricing and terms)
- Customer and supplier information
- Merger and acquisition plans
- Financials, revenues, P&L, R&D budgets

With the rise of identity fraud and other related offences, the theft of proprietary company information and private personnel records is also increasing. The records sought include:

- Home addresses
- Home phone number
- Names of spouse and children
- Employee's salary
- Social security number
- Medical records
- Credit records or credit union account information

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Performance review

Investigating Trademark and Copyright Infringement

The primary goal of this section is to impart the required knowledge of trademark and copyright issues and investigative techniques to the reader. The following key areas will be addressed in this section. It addresses how trademark and copyright infringement happens and how to put a stop to it. Additionally, the laws and definitions of patent and domain name infringement are included.

What is a "Trademark"

The United State Patient and Trade Mark Office (www.uspto.gov) states that "a trademark is a word, phrase, symbol or design, or a combination of words, phrases, symbols or designs, which identifies and distinguishes the source of the goods of one party from those of others". This definition includes brand names, symbols, slogans, a design of merchandise – even the packaging style, specific words, smell, specific color, or a amalgamation of any of the above which could aid the consumer in differentiating a particular product or service from others in an equivalent trade are categorized as trademarks. Trademarks can be fall into three primary categories, service marks, collective marks and certification marks.

Service Mark

The United State Patient and Trade Mark Office defines "a service mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce, to identify and distinguish the services of one provider from services provided by others, and to indicate the source of the services". It is comparable to a trademark with the single distinction being that a service mark is used to identify and differentiate the service of an organization from others in the equivalent field of trade.

Collective Mark

The United State Patient and Trade Mark Office defines "a collective mark is a trademark or service mark used or intended to be used, in commerce, by the members of a cooperative, an association, or other collective group or organization, including a mark, which indicates membership in a union, an association, or other organization."

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Certification Mark

The United State Patient and Trade Mark Office defines states that a "certification mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce with the owner's permission by someone other than its owner, to certify regional or other geographic origin, material, mode of manufacture, quality, accuracy, or other characteristics of someone's goods or services, or that the work or labor on the goods or services was performed by members of a union or other organization".

Service Mark and Trade Dress

The difference between a trademark and a service mark is minor. Primarily, the differentiation occurs as one of product and service. A trademark (TM is used to represent an unregistered trademark) differentiates products of the same trade. A service mark (using the symbol SM for an unregistered service mark) differentiates services of the same trade. A trademark does not only consist of a label, logo or other identifying symbol, it may also cover the distinctive packaging belonging to a particular product (e.g. the shape of a Coke bottle).

This is called Trade dress. Color pattern, shape, design, arrangement of letters/words, packaging style, and graphical presentation form a part of trade dress. In early days, trade dress referred to the way a product was packaged to be launched in the market, but now even the product design is an inclusion element of trade dress. Elements of trade dress for a particular product does not affect the way in which the product is used. Federal law for trademark applies to trade dress also. There is no distinction between trade dress and trademark, as the Lanham Act (also known as the "Trademark Act of 1946") does not provide any distinction between the two.

Trademark Eligibility and the Benefits of Registering

Any Individual or Organization who wishes to use a unique identifier in order to categorize its goods or services can qualify for a trademark. The trademark needs to be unique and not misleading. To register a trademark, the application form should be filled at the United State Patient and Trade Mark Office (USPTO).

Before the USPTO will accept an application to register a trademark, it must detail the following:

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- The applicant's name
- A name and address required for correspondence
- An apparent depiction of the mark
- A list of the goods or services provided

The applicant must also pay the application-filing fee for one or more sets of goods or services. The following points cover the benefits of registering a trademark:

- Protects an organization's name/logo,
- The registered owner attains exclusive rights of the mark and gains protection against trademark infringement.
- The mark may be used to give more visibility to the product from other products in the same trade.
- Following the trademark registration it is updated in the trademark search database, which aids in the discouraging of other applicants from filing a comparable variety of trademark.
- If a registered trademark is infringed, the title-holder of the registered trademark can request that the infringing party pay damages.
- Provides a foundation for filing the registration for the specific trademark in a foreign country.

Trademark Infringement

A trademark infringement refers to the unauthorized use of a protected trademark or service mark, or use of something very similar to a protected mark. The success of any legal action to stop (or injucnt) the infringement is directly related to whether the defendant's use of the mark causes a likelihood of confusion in the average consumer. If a court determines that a reasonable average consumer would be confused then the owner of the original mark can prevent the other party from making use of the infringing mark and even possibly collect damages. A party that holds the legal rights to a particular trademark can sue other parties for trademark infringement based on the standard "likelihood of confusion".

In the US, the Trademark Act of 1946, statutes § 1114 and § 1125 are specific to trademark infringement.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Trademark Act of 1946 ("Lanham Act") as Amended

PUBLIC LAW 79-489, CHAPTER 540, APPROVED JULY 5, 1946; 60 STAT. 427

§ 32 (15 U.S.C. §1114). Remedies; infringement; innocent infringers

(1) Any person who shall, without the consent of the registrant--

(a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or

(b) reproduce, counterfeit, copy or colorably imitate a registered mark and apply such reproduction, counterfeit, copy or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive, shall be liable in a civil action by the registrant for the remedies hereinafter provided. Under subsection (b) hereof, the registrant shall not be entitled to recover profits or damages unless the acts have been committed with knowledge that such imitation is intended to be used to cause confusion, or to cause mistake, or to deceive. As used in this paragraph, the term "any person" includes the United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, or other persons acting for the United States and with the authorization and consent of the United States, and any State, any instrumentality of a State, and any officer or employee of a State or instrumentality of a State acting in his or her official capacity. The United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, other persons acting for the United States and with the authorization and consent of the United States, and any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this Act in the same manner and to the same extent as any nongovernmental entity.

(2) Notwithstanding any other provision of this Act, the remedies given to the owner of a right infringed under this Act or to a person bringing an action under section 43(a) or (d) shall be limited as follows:

(A)

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Where an infringer or violator is engaged solely in the business of printing the mark or violating matter for others and establishes that he or she was an innocent infringer or innocent violator, the owner of the right infringed or person bringing the action under section 43(a) shall be entitled as against such infringer or violator only to an injunction against future printing.

(B)

Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510(12) of title 18, United States Code, the remedies of the owner of the right infringed or person bringing the action under section 43(a) as against the publisher or distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.

(C)

Injunctive relief shall not be available to the owner of the right infringed or person bringing the action under section 43(a) with respect to an issue of a newspaper, magazine, or other similar periodical or an electronic communication containing infringing matter or violating matter where restraining the dissemination of such infringing matter or violating matter in any particular issue of such periodical or in an electronic communication would delay the delivery of such issue or transmission of such electronic communication after the regular time for such delivery or transmission, and such delay would be due to the method by which publication and distribution of such periodical or transmission of such electronic communication is customarily conducted in accordance with sound business practice, and not due to any method or device adopted to evade this section or to prevent or delay the issuance of an injunction or restraining order with respect to such infringing matter or violating matter.

(D)(i)

(I) A domain name registrar, a domain name registry, or other domain name registration authority that takes any action described under clause (ii) affecting a domain name shall not be liable for monetary relief or, except as provided in

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

subclause (II), for injunctive relief, to any person for such action, regardless of whether the domain name is finally determined to infringe or dilute the mark.
(II) A domain name registrar, domain name registry, or other domain name registration authority described in subclause (I) may be subject to injunctive relief only if such registrar, registry, or other registration authority has--
(aa) not expeditiously deposited with a court, in which an action has been filed regarding the disposition of the domain name, documents sufficient for the court to establish the court's control and authority regarding the disposition of the registration and use of the domain name;
(bb) transferred, suspended, or otherwise modified the domain name during the pendency of the action, except upon order of the court; or
(cc) willfully failed to comply with any such court order.
(ii) An action referred to under clause (i)(I) is any action of refusing to register, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name-- (I) in compliance with a court order under section 43(d); or
(II) in the implementation of a reasonable policy by such registrar, registry, or authority prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark.
(iii) A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name.
(iv) If a registrar, registry, or other registration authority takes an action described under clause (ii) based on a knowing and material misrepresentation by any other person that a domain name is identical to, confusingly similar to, or dilutive of a mark, the person making the knowing and material misrepresentation shall be liable for any damages, including costs and attorney's fees, incurred by the domain name registrant as a result of such action. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant.
(v) A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy described under clause (ii)(II) may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

name by such registrant is not unlawful under this Act. The court may grant injunctive relief to the domain name registrant, including the reactivation of the domain name or transfer of the domain name to the domain name registrant.

(E)

As used in this paragraph--

(i) the term "violator" means a person who violates section 43(a); and

(ii) the term "violating matter" means matter that is the subject of a violation under section 43(a).

TITLE 15 > CHAPTER 22 > SUBCHAPTER III > § 1125

§ 1125. False designations of origin, false descriptions, and dilution forbidden

(a) Civil action

(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—

(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,

shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

(2) As used in this subsection, the term "any person" includes any State, instrumentality of a State or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this chapter in the same manner and to the same extent as any nongovernmental entity.

(3) In a civil action for trade dress infringement under this chapter for trade dress not registered on the principal register, the person who asserts trade dress

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

protection has the burden of proving that the matter sought to be protected is not functional.

(b) Importation

Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States. The owner, importer, or consignee of goods refused entry at any customhouse under this section may have any recourse by protest or appeal that is given under the customs revenue laws or may have the remedy given by this chapter in cases involving goods refused entry or seized.

(c) Remedies for dilution of famous marks

(1) The owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection. In determining whether a mark is distinctive and famous, a court may consider factors such as, but not limited to—

(A) the degree of inherent or acquired distinctiveness of the mark;

(B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;

(C) the duration and extent of advertising and publicity of the mark;

(D) the geographical extent of the trading area in which the mark is used;

(E) the channels of trade for the goods or services with which the mark is used;

(F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought;

(G) the nature and extent of use of the same or similar marks by third parties; and

(H) whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(2) In an action brought under this subsection, the owner of the famous mark shall be entitled only to injunctive relief as set forth in section 1116 of this title unless the person against whom the injunction is sought willfully intended to trade on the owner's reputation or to cause dilution of the famous mark. If such willful intent is proven, the owner of the famous mark shall also be entitled to the remedies set forth in sections 1117 (a) and 1118 of this title, subject to the discretion of the court and the principles of equity.

(3) The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register shall be a complete bar to an action against that person, with respect to that mark, that is brought by another person under the common law or a statute of a State and that seeks to prevent dilution of the distinctiveness of a mark, label, or form of advertisement.

(4) The following shall not be actionable under this section:

(A) Fair use of a famous mark by another person in comparative commercial advertising or promotion to identify the competing goods or services of the owner of the famous mark.

(B) Noncommercial use of a mark.

(C) All forms of news reporting and news commentary.

(d) Cyberpiracy prevention

(1)

(A) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

(ii) registers, traffics in, or uses a domain name that—

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(III) is a trademark, word, or name protected by reason of section 706 of title 18 or section 220506 of title 36.

(B)

(i) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to—

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section.

(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

(C) In any civil action involving the registration, trafficking, or use of a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

(D) A person shall be liable for using a domain name under subparagraph (A) only if that person is the domain name registrant or that registrant's authorized licensee.

(E) As used in this paragraph, the term "traffics in" refers to transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.

(2)

(A) The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if—

(i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c) of this section; and

(ii) the court finds that the owner—

(I) is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1); or

(II) through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1) by—

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(aa) sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and

(bb) publishing notice of the action as the court may direct promptly after filing the action.

(B) The actions under subparagraph (A)(ii) shall constitute service of process.

(C) In an in rem action under this paragraph, a domain name shall be deemed to have its situs in the judicial district in which—

(i) the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located; or

(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.

(D)

(i) The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall—

(I) expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name to the court; and

(II) not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

(ii) The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(3) The civil action established under paragraph (1) and the in rem action established under paragraph (2), and any remedy available under either such action, shall be in addition to any other civil action or remedy otherwise applicable.

(4) The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Copyright Violations

The United Sates Copyright Office site (www.copyright.gov) defines copyright as being "*a form of protection provided by the laws of the United States (title 17, U. S. Code) to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works. Section 106 of the 1976 Copyright Act generally gives the owner of copyright the exclusive right to do and to authorize others to do the following:*

- *To reproduce the work in copies or phonorecords;*
- *To prepare derivative works based upon the work;*
- *To distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending;*
- *To perform the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works;*
- *To display the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work; and*
- *In the case of sound recordings*, to perform the work publicly by means of a digital audio transmission".*

Investigating Copyright Status

The three fundamental methods that can be used to investigate the copyright status of a particular work include:

a. Conduct an examination of the copy of a work in order to uncover any elements that necessitate being included in the copyright notice. Works published after the 1st March, 1989 do not need to have a copyright notice incorporated with the copyrighted work. As a result, the investigator must complete an extensive research exercise through the implementation of easily obtainable tools. These tools include the use of search engines to confirm the status of the copyrighted work.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

b. The investigator may go to the U.S Copyright office's online website and database (Http://www.copyright.gov/records). A search of the database may then be initiated. This technique is recommended for users who only search the database intermittently. The record search page is classified into three categories (see figure 16.1) -

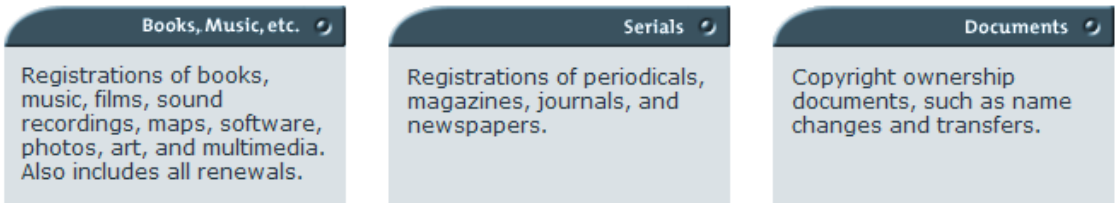
   a. Books, music etc,

   b. Serials, and

   c. Documents.

You may search a particular document after selecting the document tab. An advanced search is best conducted using the Library of Congress information System (LOCIS). The LOCIS usage guide (http://www.copyright.gov/records/guide.html) is essential reading prior to connecting to LOCIS. LOCIS runs on command prompt using either the TN3270 or Telnet protocols.

The Search Options on The U.S Copyright Office's Online Website and Database



Request the United States Copyright Office run a search against the specified category. The United State Copyright Officials will search the records for a fee of $75 per hour if a request is lodged for a copyright search. They will create either a typewritten or oral report based on the selected preference made when requesting the search.

Consider the changes to the status of copyright materials made under Copyright Act of 1976, the Berne Convention Implementation Act of 1988, the Copyright Renewal Act of 1992, and the Sonny Bono Copyright Term Extension Act of 1998 whenever you investigate copyright infringements in the US.

How Long Does a Copyright Last?

As with all things, copyright protection eventually ends; it is only a "limited monopoly." When copyrights expire, they fall into the public domain. With a number

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

of exceptions, public domain works may be unreservedly copied or used in the production of derivative works without either the permission or authorization of the former copyright holder. At some stage in the Clinton administration, the contentious "Sony Bono Copyright Term Extension Act" (CTEA) passed into law. This Act added 20 years to most copyright terms. It also created a moratorium that in effect stops any new works from entering the public domain until 2019. The Bill was enacted to ensure protection for US works in the foreign market. The CTEA includes access restrictions over works published later than 1922. The US Supreme Court rejected (ELDRED ET AL. v. ASHCROFT, ATTORNEY GENERAL 537 U.S. 186) a popular challenge to the CTEA.

Validity of copyright for joint works

Works completed by multiple (two or more) authors are called joint works. The validity of copyright for a joint work remains pending the demise of the last surviving author of the work plus an additional 70 years.

Validity of copyright for anonymous work, pseudonymous works and "made for hire" works

A copyright will remain enforce for a period of 95 years commencing in the year when the work was originally published or for a term of 120 years since the year when the work was produced. Renewal and extension of copyrights for "work for hire" works covers a term of 67 years when the owner of that particular class of work requests the extension.

The doctrine of "Fair Use"

Section 107 of the US Copyright Act details the doctrine of "*fair use*". This doctrine has evolved through the decisions of a number of court cases over time. Reproduction of a selected work for criticism, news reporting, comment, teaching, scholarship, and research is included within the provisions of "fair use" as defined in Section 107 of the Act. The Copyright Office does not provide the authorization to use copyrighted works. You need to seek permission from the owner of a particular copyrighted work.

Section 107 of the Act sets out four factors used in determining fair use:

1. The purpose and character of the use, as well as whether such use is of commercial nature or is for non-profit educational intentions,

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

2. The nature of the copyrighted work,
3. The degree and substantiality of the section used in relation to the copyrighted work as a whole, and
4. The effect of the use upon the potential market for or value of the copyrighted work.

It is difficult to distinguish amongst use that is covered by "fair use" provisions and copyright infringement. There is no mention of the number of lines, words, and notes that may be taken from a copyrighted work before it constitutes an infringement.

Copyright Violations

Copyright infringements and violations are investigated through:

a. Explanations of parties and third persons,
b. Testimonial evidences,
c. Written and material evidence,
d. Audio and video records, and
e. Conclusions of experts.

The following points list the types of evidence used to determine if a copyright violation has occurred:

- Any documents received by law enforcement agencies from the tests they completed either as a result of their own initiative or by complaints of the rights holder,
- Record of checking and searches,
- Records from the forensic examination of computer systems and software.
- Record of examination of a material carrier where the installation of software products was executed,
- Expert reports where a conclusion has been made following the assessment of the seized computer system,

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- The account of the employees of the vendor company, the account of the customer.
- Delivery note or invoice for the purchased computer system,
- Any statutory documents of a legal body,
- Job positions from the vendor selling computer facilities and software.
- Advertising materials, price lists and catalogues that provide substantiation of alleged actions,
- Warranty declaration on the purchased computer system, and
- Other documents connected to the illegal sale or distribution in any form of a copyrighted work.

At some stage in an investigation, it is essential to ascertain an estimate of the revenue obtained from an infringement or violation of a copyright and the contiguous rights.

The following financial documents should maintained as evidence:

- Reports of checks and inspections,
- Delivery notes, invoices, pick slips and other documents related to the distribution of products as well as any proof of payment,
- Financial statements and accounts,
- Agreements covering any particulars of suspected criminal activity.

How Copyright is Enforced?

The Uruguay Round Agreements Act (URAA) came into force as of the 8th December 8, 1994. This agreement introduced the Notice of Intent to Enforce (NIE). According to the URAA, the copyright holder of a restored work needs to inform the "reliance parties" if preparations to enforce copyrights for a particular work are commenced. A reliance party is an individual or organization that made use of the copyright work through its status in the public domain for the period preceding the URAA agreement.

The URAA instructs the holder of the restored work to notify the reliance party directly through the supply of a tangible notice or to present a constructive

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

notice by filing a Notice of Intent to Enforce (NIE) that is lodged with the United States Copyright Office.

A legal action may be filed against any party that is involved with a violation of the rights of the copyright holder. A party who infringes these rights but prevails upon the "fair use" doctrine in order to attempt to commercialize the work of a copyright holder by representing it as their own will often face legal action.

- The holder of a copyright that has been infringed may:
- Seek orders from a court to prevent or injunct against an escalation of infringements.
- Request compensation from the infringing party for damages, and
- Request that the infringing party pay the legal fees.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Patents and Patent Infringement

A patent is a right granted for any device, substance, method or process which is new, inventive and useful. It is essentially a monopoly right over a registered invention or discovery that is legally enforceable and provides the holder the exclusive right to commercially exploit the invention for the life of the patent. A patent is not automatic and it must be applied for and registered in each country to which it is to apply (there is no such thing as an international patent). Patents give effective protection if you have invented new technology that will lead to a product, composition or process with significant long-term commercial gain.

In the US, the Patent and Trademark Office issues patents. They are effective up to 20 years from the date on which the application is filed. In Australia and many other countries there are two types of patents in operation;

- A standard patent gives long-term protection and control over an invention for up to 20 years.
- An innovation patent is a relatively fast, inexpensive protection option, lasting a maximum of 8 years. The Australian innovation patent replaced the petty patent on 24 May 2001.

Patent laws allow for the granting of a patent on the new article not on the propositions that claim to put into practice those ideas to make the article. You cannot patent an idea.

Any article, process, or manufacturing technique that asserts a right to a patent is required to prove its utility. In 35 U.S.C. § 102, US Patent law states that invention cannot be patented where:

a. *the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent, or*

b. *the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country more than one year prior to the application for patent in the United States or*

c. *he has abandoned the invention, or*

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

d. *the invention was first patented or caused to be patented, or was the subject of an inventor's certificate, by the applicant or his legal representatives or assigns in a foreign country prior to the date of the application for patent in this country on an application for patent or inventor's certificate filed more than twelve months before the filing of the application in the United States, or….*

The primary types of patents include:

- Utility patents which are granted to an individual who ascertains or invents a new instrument, process, useful composition of matter, or manufacture. Some examples include:
- A new processes for the fraction distillation of petroleum,
- A novel manufacturing method for paper,
- A machine such as a motorbike or car,
- A previously undiscovered composition of matter including a drug.
- Design Patents are granted to an individual who creates a new, innovative design for an article of manufacture. It guards the look of an article, for example, the shape of the Apple iPod.
- Plant Patents or Breeders rights are granted to an individual who conceives, discovers, or asexually reproduces a distinctive variety of plant.
- An innovation patent which is a fast, inexpensive but limited protection option

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Patent Infringement

Patent infringement is governed in the US by federal law. 35 U.S.C. 271. This defines infringement as "whoever without authority makes, uses, or sells any patented invention, within the United States during the term of the patent therefore, infringes the patent".

Wikipedia.com, “Any party that manufactures, uses, sells, or offers for sale patented technology, during the term of the patent and within the country that issued the patent, is considered to infringe the patent. The test varies from country to country, but in general it requires that the infringer's product (or method, service, etc) falls within one or more of the claims of the granted patent. In the United States and others that use a "peripheral claiming", that means that the infringing technology embodies each and every of the elements listed in the claim. If the technology incorporates all of a claim's elements (and possibly more) it is said to "read on" the claim; if a single element from the claim is missing from the technology it does not read on the claim and thereby does not infringe the patent with respect to that claim”[1].

There are three primary categories of patent infringement. These are:

- Direct infringement. Direct by infringement occurs whenever any individual constructs, uses, offers to sell, sells, or imports into the country where the patent is held any patented invention, without authority, during the term of the patent.
- Indirect infringement. If a person instigates another person to sell, make, or use a patented invention is liable to fall under the category of indirect infringer.
- Contributory infringement. Also known as an “active inducement to infringement”, 35 U.S.C. § 271(b) states "whoever actively induces infringement of a patent shall be liable as an infringer."

Resolving patent infringement is a two-step process:

- Analysis of claims by going through all patented documents.

[1] http://en.wikipedia.org/wiki/Patent_infringement

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Verifying the claim for its authenticity. In this step, devices or processes, which are claimed, are validated to establish the accuracy of the claim.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

US Laws related to Trademark, Patient and Copyright

US Federal Statutes:

- 18 U.S.C. 1030 - Fraud and related activity in connection with computers
- 18 U.S.C. 1343 - Fraud by wire, radio, or television
- 18 U.S.C. 1361 - Injury to government property
- 18 U.S.C. 1362 - Government communication systems
- 18 U.S.C. 1831 - Economic Espionage Act
- 18 U.S.C. 1832 - Theft of trade secrets

§ 2319A. Unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances

(a) Offense. –Whoever, without the consent of the performer or performers involved, knowingly and for purposes of commercial advantage or private financial gain–

(1) Fixes the sounds or sounds and images of a live musical performance in a copy or phonorecord, or reproduces copies or phonorecords of such a performance from an unauthorized fixation;

(2) Transmits or otherwise communicates to the public the sounds or sounds and images of a live musical performance; or

(3) Distributes or offers to distribute, sells or offers to sell, rents or offers to rent, or traffics in any copy or phonorecord fixed as described in paragraph (1), regardless of whether the fixations occurred in the United States;

Shall be imprisoned for not more than 5 years or fined in the amount set forth in this title, or both, or if the offense is a second or subsequent offense, shall be imprisoned for not more than 10 years or fined in the amount set forth in this title, or both.

(b) Forfeiture and destruction. —When a person is convicted of a violation of subsection (a), the court shall order the forfeiture and destruction of any copies or phonorecords created in violation thereof, as well as any plates, molds, matrices,

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

masters, tapes, and film negatives by means of which such copies or phonorecords may be made. The court may also, in its discretion, order the forfeiture and destruction of any other equipment by means of which such copies or phonorecords may be reproduced, taking into account the nature, scope, and proportionality of the use of the equipment in the offense.

(C) Seizure and forfeiture. —If copies or phonorecords of sounds or sounds and images of a live musical performance are fixed outside of the United States without the consent of the performer or performers involved, such copies or phonorecords are subject to seizure and forfeiture in the United States in the same manner as property imported in violation of the customs laws. The Secretary of the Treasury shall, not later than 60 days after the date of the enactment of the Uruguay Round Agreements Act, issue regulations to carry out this subsection, including regulations by which any performer may, upon payment of a specified fee, be entitled to notification by the United States Customs Service of the importation of copies or phonorecords that appear to consist of unauthorized fixations of the sounds or sounds and images of a live musical performance.

(d) Victim impact statement. —

(1) During preparation of the presentence report pursuant to Rule 32© of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements should include—

(A) Producers and sellers of legitimate works affected by conduct involved in the offense;

(B) Holders of intellectual property rights in such works; and

(C) The legal representatives of such producers, sellers, and holders.

(e) Definitions. —As used in this section—

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(1) The terms "copy," "fixed," "musical work," "phonorecord," "reproduce," "sound recordings," and "transmit" mean those terms within the meaning of title 17; and

(2) The term "traffic in" means transport, transfer, or otherwise dispose of, to another, as consideration for anything of value, or make or obtain control of with intent to transport, transfer, or dispose of.

(f) Applicability. —This section shall apply to any Act or Acts that occur on or after the date of the enactment of the Uruguay Round Agreements Act.

§ 2320. Trafficking in counterfeit goods or services

(a) Whoever intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services shall, if an individual, be fined not more than $2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, be fined not more than $5,000,000. In the case of an offense by a person under this section that occurs after that person is convicted of another offense under this section, the person convicted, if an individual, shall be fined not more than $5,000,000 or imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than $15,000,000.

(b) Upon a determination by a preponderance of the evidence that any articles in the possession of a defendant in a prosecution under this section bear counterfeit marks, the United States may obtain an order for the destruction of such articles.

(C) All defenses, affirmative defenses, and limitations on remedies that would be applicable in an action under the Lanham Act shall be applicable in a prosecution under this section. In a prosecution under this section, the defendant shall have the burden of proof, by a preponderance of the evidence, of any such affirmative defense.

(d)

(1) During preparation of the presentence report pursuant to Rule 32© of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements should include—

(A) Producers and sellers of legitimate goods or services affected by conduct involved in the offense;

(B) Holders of intellectual property rights in such goods or services; and

(C) The legal representatives of such producers, sellers, and holders.

(e) For the purposes of this section—

(1) The term "counterfeit mark" means—

(A) A spurious mark—

(i) That is used in connection with trafficking in goods or services;

(ii) That is identical with, or substantially indistinguishable from, a mark registered for those goods or services on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered; and

(iii) The use of which is likely to cause confusion, to cause mistake, or to deceive; or

(B) A spurious designation that is identical with, or substantially indistinguishable from, a designation as to which the remedies of the Lanham Act are made available by reason of section 220506 of title 36; but such term does not include any mark or designation used in connection with goods or services of which the manufacturer or producer was, at the time of the manufacture or production in question authorized to use the mark or designation for the type of goods or services so manufactured or produced, by the holder of the right to use such mark or designation;

(2) The term "traffic" means transport, transfer, or otherwise dispose of, to another, as consideration for anything of value, or make or obtain control of with intent so to transport, transfer, or dispose of; and

(3) The term "Lanham Act" means the Act entitled "An Act to provide for the registration and protection of trademarks used in commerce, to carry out the

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

provisions of certain international conventions, and for other purposes," approved July 5, 1946 (15 U.S.C. 1051 et seq.).

(f)

(1) Beginning with the first year after the date of enactment of this subsection, the Attorney General shall include in the report of the Attorney General to Congress on the business of the Department of Justice prepared pursuant to section 522 of title 28, an accounting, on a district by district basis, of the following with respect to all actions taken by the Department of Justice that involve trafficking in counterfeit labels for phonorecords, copies of computer programs or computer program documentation or packaging, copies of motion pictures or other audiovisual works (as defined in section 2318 of this title), criminal infringement of copyrights (as defined in section 2319 of this title), unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances (as defined in section 2319A of this title), or trafficking in goods or services bearing counterfeit marks (as defined in section 2320 of this title):

(A) The number of open investigations.

(B) The number of cases referred by the United States Customs Service.

(C) The number of cases referred by other agencies or sources.

(D) The number and outcome, including settlements, sentences, recoveries, and penalties, of all prosecutions brought under sections 2318, 2319, 2319A, and 2320 of this title.

(2)

(A) The report under paragraph (1), with respect to criminal infringement of copyright, shall include the following:

(i) The number of infringement cases in these categories: audiovisual (videos and films); audio (sound recordings); literary works (books and musical compositions); computer programs; video games; and, others.

(ii) The number of online infringement cases.

(iii) The number and dollar amounts of fines assessed in specific categories of dollar amounts. These categories shall be: no fines ordered; fines under $500; fines

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

from $500 to $1,000; fines from $1,000 to $5,000; fines from $5,000 to $10,000; and fines over $10,000.

(iv) The total amount of restitution ordered in all copyright infringement cases.

(B) In this paragraph, the term "online infringement cases" as used in paragraph (2) means those cases where the infringer—

(i) Advertised or publicized the infringing work on the Internet; or

(ii) Made the infringing work available on the Internet for download, reproduction, performance, or distribution by other persons.

(C)The information required under subparagraph (A) shall be submitted in the report required in fiscal year 2005 and thereafter.

§ 1831. Economic espionage

(a) In general. —Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) Steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) Attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) Conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) Organizations. —Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

§ 1832. Theft of trade secrets

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) Steals, or without authorization appropriates takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) Receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) Attempts to commit any offense described in paragraphs (1) through (3); or

(5) Conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000

§ 1833. Exceptions to prohibitions

This chapter does not prohibit—

(1) Any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

(2) The reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

§ 1834. Criminal forfeiture

(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States—

(1) Any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(2) Any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this section.

§ 1835. Orders to preserve confidentiality

In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

§ 1836. Civil proceedings to enjoin violations

(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this chapter.

(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this section.

§ 1837. Applicability to conduct outside the United States

This chapter also applies to conduct occurring outside the United States if—

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(1) The offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

(2) An act in furtherance of the offense was committed in the United States.

§ 1838. Construction with other laws

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

§ 1839. Definitions

(1) The term "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

(2) The term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

(3) The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) The owner thereof has taken reasonable measures to keep such information secret; and

(B) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

(4) The term "owner," with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(C) Fraudulent Copyright Notice. —Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than $2,500.

(d) Fraudulent Removal of Copyright Notice. —Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than $2,500.

§ 497. Letters patent

Whoever falsely makes, forges, counterfeits, or alters any letters patent granted or purporting to have been granted by the President of the United States; or Whoever passes, utters, or publishes, or attempts to pass, utter, or publish as genuine, any such letters patent, knowing the same to be forged, counterfeited or falsely altered— Shall be fined under this title or imprisoned not more than ten years, or both.

§ 292. False marking

(a) Whoever, without the consent of the patentee, marks upon, or affixes to, or uses in advertising in connection with anything made, used, offered for sale, or sold by such person within the United States, or imported by the person into the United States, the name or any imitation of the name of the patentee, the patent number, or the words "patent," "patentee," or the like, with the intent of counterfeiting or imitating the mark of the patentee, or of deceiving the public and inducing them to believe that the thing was made, offered for sale, sold, or imported into the United States by or with the consent of the patentee; or

Whoever marks upon, or affixes to, or uses in advertising in connection with any unpatented article, the word "patent" or any word or number importing that the same is patented for the purpose of deceiving the public; or

Whoever marks upon, or affixes to, or uses in advertising in connection with any article, the words "patent applied for," "patent pending," or any word importing that an application for patent has been made, when no application for patent has been made, or if made, is not pending, for the purpose of deceiving the public—

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Shall be fined not more than $500 for every such offense.

(b) Any person may sue for the penalty, in which event one-half shall go to the person suing and the other to the use of the United States.

§ 1341. Frauds and swindles

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives there from, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

§ 1343. Fraud by wire, radio, or television

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

§ 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication-intercepting devices prohibited

(1)Except as otherwise specifically provided in this chapter, any person who intentionally—

(a) Sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) Manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(C) Places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of—

(i) Any electronic, mechanical, or other device knowing the content of the advertisement and knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) Any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) A provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(b) An officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

§ 553. Unauthorized reception of cable service

(a) Unauthorized interception or receipt or assistance in intercepting or receiving service; "assist in intercepting or receiving" defined

(1) No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law.

(2) For the purpose of this section, the term "assist in intercepting or receiving" shall include the manufacture or distribution of equipment intended by the manufacturer or distributor (as the case may be) for unauthorized reception of any communications service offered over a cable system in violation of subparagraph (1).

(b) Penalties for willful violation

(1) Any person who willfully violates subsection (a)(1) of this section shall be fined not more than $1,000 or imprisoned for not more than 6 months, or both.

(2) Any person who violates subsection (a)(1) of this section willfully and for purposes of commercial advantage or private financial gain shall be fined not more than $50,000 or imprisoned for not more than 2 years, or both, for the first such

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

offense and shall be fined not more than $100,000 or imprisoned for not more than 5 years, or both, for any subsequent offense.

(3) For purposes of all penalties and remedies established for violations of subsection (a)(1) of this section, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation.

(C) Civil action in district court; injunctions; damages; attorney's fees and costs; regulation by States or franchising authorities

(1) Any person aggrieved by any violation of subsection (a)(1) of this section may bring a civil action in a United States district court or in any other court of competent jurisdiction.

(2) The court may—

(A) Grant temporary and final injunctions on such terms, as it may deem reasonable to prevent or restrain violations of subsection (a) (1) of this section;

(B) Award damages as described in paragraph (3); and

(C) Direct the recovery of full costs, including awarding reasonable attorneys' fees to an aggrieved party who prevails.

(3)

(A) Damages awarded by any court under this section shall be computed in accordance with either of the following clauses:

(i) The party aggrieved may recover the actual damages suffered by him as a result of the violation and any profits of the violator that are attributable to the violation which are not taken into account in computing the actual damages; in determining the violator's profits, the party aggrieved shall be required to prove only the violator's gross revenue, and the violator shall be required to prove his deductible expenses and the elements of profit attributable to factors other than the violation; or

(ii) The party aggrieved may recover an award of statutory damages for all violations involved in the action, in a sum of not less than $250 or more than $10,000 as the court considers just.

(B) In any case in which the court finds that the violation was committed willfully and for purposes of commercial advantage or private financial gain, the

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

court in its discretion may increase the award of damages, whether actual or statutory under subparagraph (A), by an amount of not more than $50,000.

(C) In any case where the court finds that the violator was not aware and had no reason to believe that his acts constituted a violation of this section, the court in its discretion may reduce the award of damages to a sum of not less than $100.

(D) Nothing in this subchapter shall prevent any State or franchising authority from enacting or enforcing laws, consistent with this section, regarding the unauthorized interception or reception of any cable service or other communications service.

§ 605. Unauthorized publication or use of communications

(a)Practices prohibited

Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception,

(1) to any person other than the addressee, his agent, or attorney,

(2) to a person employed or authorized to forward such communication to its destination,

(3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed,

(4) to the master of a ship under whom he is serving,

(5) in response to a subpoena issued by a court of competent jurisdiction, or

(6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance,

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.

(b)Exceptions

The provisions of subsection (a) of this section shall not apply to the interception or receipt by any individual, or the assisting (including the manufacture or sale) of such interception or receipt, of any satellite cable programming for private viewing if—

(1) The programming involved is not encrypted; and

(2)

(A) a marketing system is not established under which—

(i) An agent or agents have been lawfully designated for the purpose of authorizing private viewing by individuals, and

(ii) Such authorization is available to the individual involved from the appropriate agent or agents; or

(B) A marketing system described in subparagraph (A) is established and the individuals receiving such programming have obtained authorization for private viewing under that system.

(c) Scrambling of Public Broadcasting Service programming

No person shall encrypt or continue to encrypt satellite delivered programs included in the National Program Service of the Public Broadcasting Service and intended for public viewing by retransmission by television broadcast stations; except that as long as at least one unencrypted satellite transmission of any program subject to this subsection is provided, this subsection shall not prohibit additional encrypted satellite transmissions of the same program.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(d) Definitions

For purposes of this section—

(1) The term "satellite cable programming" means video programming which is transmitted via satellite and which is primarily intended for the direct receipt by cable operators for their retransmission to cable subscribers;

(2) The term "agent," with respect to any person, includes an employee of such person;

(3) The term "encrypt," when used with respect to satellite cable programming, means to transmit such programming in a form whereby the aural and visual characteristics (or both) are modified or altered for the purpose of preventing the unauthorized receipt of such programming by persons without authorized equipment which is designed to eliminate the effects of such modification or alteration;

(4) The term "private viewing" means the viewing for private use in an individual's dwelling unit by means of equipment, owned or operated by such individual, capable of receiving satellite cable programming directly from a satellite;

(5) The term 'private financial gain" shall not include the gain resulting to any individual for the private use in such individual's dwelling unit of any programming for which the individual has not obtained authorization for that use; and

(6) The term "any person aggrieved" shall include any person with proprietary rights in the intercepted communication by wire or radio, including wholesale or retail distributors of satellite cable programming, and, in the case of a violation of paragraph (4) of subsection (e) of this section shall also include any person engaged in the lawful manufacture, distribution, or sale of equipment necessary to authorize or receive satellite cable programming.

(e) Penalties; civil actions; remedies; attorney's fees and costs; computation of damages; regulation by State and local authorities

(1) Any person who willfully violates subsection (a) of this section shall be fined not more than $2,000 or imprisoned for not more than 6 months, or both.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(2) Any person who violates subsection (a) of this section willfully and for purposes of direct or indirect commercial advantage or private financial gain shall be fined not more than $50,000 or imprisoned for not more than 2 years, or both, for the first such conviction and shall be fined not more than $100,000 or imprisoned for not more than 5 years, or both, for any subsequent conviction.

(3)

(A) Any person aggrieved by any violation of subsection (a) of this section or paragraph (4) of this subsection may bring a civil action in a United States district court or in any other court of competent jurisdiction.

(B) The court—

(i) May grant temporary and final injunctions on such terms, as it may deem reasonable to prevent or restrain violations of subsection (a) of this section;

(ii) May award damages as described in subparagraph ©; and

(iii) Shall direct the recovery of full costs, including awarding reasonable attorneys' fees to an aggrieved party who prevails.

(c)

(i) Damages awarded by any court under this section shall be computed, at the election of the aggrieved party, in accordance with either of the following subclasses;

(I) The party aggrieved may recover the actual damages suffered by him as a result of the violation and any profits of the violator that are attributable to the violation which are not taken into account in computing the actual damages; in determining the violator's profits, the party aggrieved shall be required to prove only the violator's gross revenue, and the violator shall be required to prove his deductible expenses and the elements of profit attributable to factors other than the violation; or

(II) The party aggrieved may recover an award of statutory damages for each violation of subsection (a) of this section involved in the action in a sum of not less than $1,000 or more than $10,000, as the court considers just, and for each violation of paragraph (4) of this subsection involved in the action an aggrieved party may recover statutory damages in a sum not less than $10,000, or more than $100,000, as the court considers just.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

(ii) In any case in which the court finds that the violation was committed willfully and for purposes of direct or indirect commercial advantage or private financial gain, the court in its discretion may increase the award of damages, whether actual or statutory, by an amount of not more than $100,000 for each violation of subsection (a) of this section.

(iii) In any case where the court finds that the violator was not aware and had no reason to believe that his acts constituted a violation of this section, the court in its discretion may reduce the award of damages to a sum of not less than $250.

(4) Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a) of this section, shall be fined not more than $500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both. For purposes of all penalties and remedies established for violations of this paragraph, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation.

(5) The penalties under this subsection shall be in addition to those prescribed under any other provision of this subchapter.

(6) Nothing in this subsection shall prevent any State, or political subdivision thereof, from enacting or enforcing any laws with respect to the importation, sale, manufacture, or distribution of equipment by any person with the intent of its use to assist in the interception or receipt of radio communications prohibited by subsection (a) of this section.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Bibliography

1. Argy, Phillip (2006) "Electronic Evidence, Document Retention and Privacy" Australian Corporate Lawyers' Association (ACLA) NSW Annual Conference, Sydney, 30-31 March 2006
2. Boni, William & Kovacich, Gerald L. (2000) "Netspionage: The Global Threat to Information" Butterworth-Heinemann
3. Chua, Wai Fong & Toorn, Christine Van (2005) "DOCUMENTS, RISK AND THE FATE OF YOUR ORGANISATION, Document management in the age of corporate accountability" 9 November 2005, University of New South Wales
4. CSI, the Computer Security Institute. Web site at http://www.gocsi.com/
5. Harris, Shon (2003). "*All-in-One CISSP Certification Exam Guide*", 2nd Edition. Emeryville, CA: McGraw-Hill/Osborne. (0-07-222966-7)
6. Mokhiber, Russell & Weissman, Robert. (2001) "Corporate Spooks." 6th Mar 2001. http://www.commondreams.org/views01/0306-03.htm (02 Aug 07)
7. Nichols, Randall K., Ryan, Daniel J. & Ryan, Julie J.C.H. (2000) "Introduction to Digital Espionage, Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves" McGraw-Hill
8. NSoPE (National Society of Professional Engineers), (2005) "*Document Retention Guidelines*" PROFESSIONAL ENGINEERS IN PRIVATE PRACTICE DIVISION Professional Liability Committee, March 2005
9. Rich, Lloyd L. (2006) "*Right to Privacy in the Workplace in the Information Age*." http://www.publaw.com/privacy.html
10. WarRoom, (1996) "1996 Information Systems Security Survey" WarRoom Research, LLC, available at http://www.infowar.com/
11. Zwillinger, Marc J., (1998) "Investigation and Prosecution of Computer Crime," Computer Crime and Intellectual Property Section Criminal Division, U.S. Department of Justice, 4 November 1998,

Cases

1. *British American Tobacco Australia Services Limited v Roxanne Joy Cowell* for the estate of *Rolah Ann McCabe [2002] VSCA 197*
2. **Infabrics Ltd. v. Jaytex Ltd., [1982] AC 1 (HL);**
3. *Residential Funding Corp. v. DeGeorge Fin. Corp. 306 F.3d 99*

Statues and Regulations

1. Electronic Transactions Act, 1999
2. Evidence Act 1995
3. Freedom of Information Act 1982
4. Archives Act 1983

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5. The Gramm-Leach-Bliley Act: The Financial Privacy Rule. Federal Trade Commission. http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html
6. Income Tax Assessment Act 1997
7. A New Tax System (Goods and Services Tax) Act 1999
8. A New Tax System (Fringe Benefits) Act 1999
9. Corporations Act 2001
10. Privacy Act 1988
11. Workplace Relations Act 1996

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Standards and Other Guidelines

The standards and other resources referenced in the paper.

Standards

BS 4783
Storage, transportation and maintenance of media for use in data processing and information storage (in several parts)

BS 7978
Bundles for the Perpetual Preservation of electronic documents and associated objects

ISO 639
Codes for the representation of names of languages

ISO 3166
Codes for the representation of names of countries

ISO 8601
Data elements and interchange formats – Information interchange – Representation of dates and times

ISO 8859
Information technology – 8-bit single-byte coded graphic character sets

ISO 9075
Information technology – database languages – SQL

ISO 10646
Information technology – Universal Multiple-Octet Coded Character Set

ISO 23950
Information retrieval – application service definition and protocol specification

Other Guidelines

90/270/EEC
European Commission "Display Screen Equipment Directive"

BSI DISC PD 0008
Code of Practice for the Legal Admissibility and Evidential Weight of Information Stored Electronically

Accessibility Guidelines

SPRITE-S2 initiative
ACCENT – Accessibility in ICT Procurement
(http://www.statskontoret.se/accenteng.htm)

W3C Web Content Accessibility Guidelines
(http://www.w3.org/TR/WAI-WEBCONTENT)

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Microsoft Official Guidelines for User Interface Developers and Designers
Chapter 15, Special Design Considerations, Accessibility
(http://msdn.microsoft.com/library/books/winguide/ch15c.htm)

Guidelines for Long Term Preservation

InterPARES project (http://www.interpares.org)

Preserving Access to Digital Information (PADI) project
National Library of Australia (http://www.nla.gov.au/padi/)

UK Public Record Office
Management, Appraisal and Preservation of Electronic Records Guidelines.
(http://www.pro.gov.uk/recordsmanagement/eros/guidelines/default.htm)

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced