These materials are presented for general educational purposes only. These materials are not suitable for and may not be relied upon for resolving issues or giving advice concerning particular legal matters. Individuals seeking advice concerning any particular legal matters relating to or concerning issues discussed in these materials are strongly advised to consult with a knowledgeable attorney concerning such particular legal matters. These materials concern a rapidly evolving area of the law and only deal with certain aspects of that area of law. Any person researching particular legal matters relating to or concerning issues discussed in these materials is cautioned to refer to and review original legal source materials thoroughly and to look for recent changes or additions to such materials as part of such research.

An Internet Primer
The Law of the Internet in California Seminar
National Business Institute - May 31, 2001

Michael Risch, Jack Russo, and John Kelley/
Russo & Hale LLP
computerlaw.com℠

I. Introduction

In 1969, the Advance Research Projects Agency (ARPA) launched a government funded network called ARPAnet, and the global computer network has never been the same.[1] The goal of the ARPAnet (and its successors) was to create an internetwork of computers within the government and research universities. There were two primary requirements: 1) the network had to be **robust,** and 2) the network had to be **standardized**. The end result after many years of development was a network based on TCP/IP (Transport Control Protocol/Internet Protocol), which was adopted as a standard in 1983.[2]

To create a robust network, the TCP/IP "packets" are designed to be "routable". That is, the packets are sent from each network segment (for example a department or a school) through a series of routers that each have a connection to several other routers. If

---

[1]For a complete history and description of the internet, some good sources are Where Wizards Stay Up Late: The Origins of the Internet, by Katie Hafner and Matthew Lyon, Simon and Schuster (1996) and The Pocket Internet, by Sean Greer, Economist Books (2000).

[2]To be truly historically accurate, we note that TCP came first, and it wasn't combined with IP for many years.

one router is unavailable (say, due to war or just plain unreliability), then the packet would still be delivered via a different router and route.

To create a standardized network, TCP/IP was designed to be computer and network independent. So long as the information is encapsulated in a standard TCP/IP packet, it can be processed by any other computer running a "TCP/IP Stack," regardless of type.

As time passed, this network grew and became globalized and commercial, which is the internet we know today. This section discusses the basics of the internet and some of the key lingo used. The glossary of terms is organized on a functional level, so that you can both learn how the internet works while learning key terms. Even if you are familiar with the internet, you should review this section, as the various pieces of the internet generate key areas to consider in legal analysis.

II. The Basics

The internet works using a variety of different layers:

MAC Address: Every network device (such as an ethernet card) has a unique MAC (Machine Address Code). This is the only and only way to identify the network device on the network.

Hardware Layer: This is the term often used to describe the communication standard used by specific types of network devices. Common hardware layers are ethernet, fiber optics, broadband, and token ring.

IP: This is what makes the internet go - the Internet Protocol (used interchangeably with TCP/IP, though there are technical differences). Information on the

hardware layer is encapsulated into IP packets, which can be decoded by any other network device that understands IP packets, even if they use a different hardware layer.

IP Address: This is the address that ties to the MAC Address for any given network device. Unlike the MAC Address, the IP Address can change at any time, and more than one IP Address can be associated with a MAC Address. The IP Address is a four part, decimal notated number (w.x.y.z) though it can also be represented by a large number – companies sending spam have been known to use this trick to get people to open a web site.

Router: Unfortunately, it would take too many resources for every network device to know the MAC Address or IP Address of every computer on the internet. The ingenious part of IP is the ability to route. Each network device need only know the next "hop" in the line. Every network or subnetwork needs at least one router. It is usually called a "default" router. The IP Packet is sent to the default router, which then sends the packet to the next router in the line. As the size of the network provider grows, the number of router choices grows. Eventually, the IP Packet arrives at the default router for the receiving network. That router knows the IP Addresses and the corresponding MAC Addresses for the computers on that network and delivers the packet to its destination.

Subnet and **Network Class**: It would be pretty inefficient for each router to know each and every IP Address on the subnetwork. For this reason, IP Addresses are assigned in groups, where many of the numbers are the same. For example, 192.168.1.10 and 192.168.1.20 are two computers on the same "Class C" subnet. 192.168.1.10 and 192.168.10.10 are on a "Class B" subnet. Finally, 192.168.1.10 and 192.169.1.10 are on

the same “Class A” subnet. So long as all the network devices on the subnet know what type of subnet it resides on, they can all communicate. In fact, subnets can be reduced down to as few as 2 IP Addresses. As the number of IP Address available dwindles, the subnets assigned are getting smaller and smaller. This was not a concern at the beginning of the internet - Stanford University has a class A subnet, which is the same number of IP Addresses given to many small countries.

Now, here’s where subnets help routers. Rather than needing to know and broadcast to other routers each IP Address on the subnet, a router only needs to broadcast the network. That means that Stanford’s routers need only broadcast 171.0.0.0 and every IP Packet addressed to one of the Class A subnet IP Addresses will be sent to those routers. Even within a company, departments may assign different subnets and separate them with routers in order to reduce network traffic - IP Packets not bound for an “outside” subnet will not be routed.

Another reason why computers on a network cannot be given random IP Addresses is that the chance of duplicated IP Addresses would increase, and each IP Address can only be used once on a network, even one as large as the internet.

Switch: In the description of routers, above, the router is described as “delivering” the IP Packet. This is not really true in practice. Instead, a standard router will “broadcast” the packets over the network and the network device that owns the correct address will claim it. This can get inefficient as more data and more computers are added to the network. A network switch keeps track of which computer (or set of computers) is hooked up to each “port” of the switch, and will send IP traffic only to the network

segment that holds the appropriate network device. Note that subnets are still necessary, as switches handle less traffic than routers.

Firewall: A firewall is a device that blocks incoming or outgoing network traffic, to either limit use or secure a network from outside intruders. Some firewalls offer a "VPN" or "Virtual Private Network" which is an secure private connection into a network from outside of the firewall.

Some firewalls perform network address translation, or "NAT". In this process, the firewall presents a single IP Address to the world, and each of the internal IP Addresses share the single external address. This further secures the internal network because intruders cannot "find" any specific internal machine. An additional benefit is that internal IP Addresses can be duplicates of other IP Addresses on the internet - as the number of computers proliferates, NAT can be used to reduce the number of IP Addresses used.

Domain Name: It would be impossible for people to remember every company's IP Address, for use in such things as world wide web connections and sending email. Thankfully, "domain names" and "host names" can be used as monikers to represent a set of IP Addresses or a single IP Address respectively. For example, with *www.computerlaw.com*, the ".com" describes the type of domain it is (commercial), "computerlaw.com" describes a set of IP Addresses assigned to Russo & Hale LLP, and "www.computerlaw.com" identifies a specific IP Address, namely the Russo & Hale web server.

ICAAN: Domains were originally handled in the U.S. by a single organization, but has since been decentralized to a variety of competing organizations. These organizations are responsible for doling out domain names and IP Addresses, and for resolving disputes relating to domain names. Each of the domain name authorities are "managed" by the ICAAN, or the Internet Corporation for Assigned Names and Numbers. The ICAAN doles out blocks of IP Addresses to the different authorities; this is an important function – as blocks of IP Addresses become more scarce, ISP's become willing to pay more and more for them to offer to their customers. Some ISP's, for example, now refuse to give a fixed IP Address to its customers, instead forcing customers to share a pool. "Owning" a block of IP Addresses can make a company far more valuable.

The ICANN also sets domain name dispute policies that each sub-authority must agree to, and which in turn all parties registering domain names must agree to.

Domain Hierarchy: In the US here are several "top-level" domain names, each of which is intended to have meaning. There are no steadfast rules as to which must be used, but convention dictates the following:

.*com*: This term has become ubiquitous for commercial organizations on the web.

.*org*: Non-commercial organizations and associations should use these addresses.

.*gov*: These domains are reserved for the government.

.*mil*: These domains are reserved for the military.

.*net*: These domains are used primarily by network providers, though some other commercial companies have used them.

.*cc*: Another commercial designation.

Additionally, there are new and upcoming top-level domain names. These are listed at http://www.icann.org/tlds/.

III. The Modern Internet

The internet as we know it today is very different than just five or six years ago, and unrecognizable compared to ten years ago. In 1990, the primary way the internet was accessed was through "terminals" to command line based Unix (and other OS - TOPS20, VMS, etc.) computers. These terminals were just emulations of what was actually happening at the main computer - the internet was used for connectivity, but the computing power was completely centralized. A student running a complex program on multiple terminals could bring a central computer to a virtual halt.

Today, resources are far more distributed, and far more complex. Once again, an understanding of the lingo will also serve as an understanding of the modern internet.

DNS or **Domain Name Service**: This is the protocol used to match up IP Addresses with domain names. Additionally, DNS allows for a "reverse look-up" which ties a domain name to an IP address. If DNS is not configured or not working for a computer, then the domain and host name will not "resolve" to an IP Address, and the attempted activity will fail. Even if DNS does not work, however, you can often simply used the IP Address (if you know it) to achieve the same results.

Ping: This is one of the smallest and most useful test programs there is - it sends a packet (using the ICMP protocol) to a network device and reports whether a response was received. This allows testing of both the receiving device and the connection between

them. An companion program is *traceroute*, which reports each router hop from the current computer and the destination; this allows for testing of any breakdowns in the system.

Unfortunately, ping can be used for destructive purposes in a “Denial of Service” or “Ping of Death” attack. Using a variety of hijacked machines (usually through a trojan horse), a cracker will send millions of pings to a server, until the server can handle nothing else. A series of such attacks took place in 2000, bringing several of the largest web providers in the world, including Microsoft, Yahoo, and eBay to their knees.

SMTP: The Simple Mail Transfer Protocol is the primary method that electronic mail is forwarded around the internet. It is robust in its simplicity, as it is still the standard so many years after its creation. SMTP is a store and forward protocol. A mail address is sent from one mail server to another until it reaches its destination. Sometimes, that can be a single computer to another, but other times it may take many hops. If the receiving computer is not working, the sender will store the mail for a period of time (usually five days or so) or until the receiving computer is working.

Telnet: This was the primary method for accessing central computers by a terminal window. A telnet session is simply a command-line “shell” to the central computer. This is usually the Unix version of DOS prompt, though some systems offer more sophisticated programming. For example, the Library of Congress offered (and still does offer) its LOCIS menu driven system via telnet.

Usenet: The usenet[3] is a conglomeration of thousands of discussion groups relating to every topic imaginable. Users post comments or questions, and other users reply with their own comments, questions or answers.

FTP: This was the original, and for many is still, the primary file transfer protocol on the internet. One computer can connect to another computer offering FTP services, view a list of files available, and "download" one or more files.

Gopher: This was a precursor to the world wide web. It was a text based hyperlinked system of data retrieval. It and its cousin the Wide Area Information Service (WAIS) were the first successful attempt to link information on different computers together in either a searchable or hyperlinked form.

World Wide Web/WWW/HTTP: For many people, the world wide web is synonymous with the internet. How often have you heard someone say that "their internet is down" when what they really mean is that they cannot obtain world wide web access (on a side note - sometimes the "internet is down" when really all that is happened is that DNS is not properly resolving host names).

The world wide web is founded on the HyperText Transfer Protocol (HTTP). This protocol governs how world wide web servers talk to world wide web browsers. The protocol is defined by the World Wide Web Consortium (W3C).[4]

Web Browser: These computer programs serve two purposes. First, they use the

---

[3]Google has recently purchased the usenet archive on the web, at http://www.google.com.

[4]See http://www.w3.org/ for a full listing of W3C protocols.

HTTP protocol to communicate with world wide web service providers. Then, they display world wide web content received from those providers. Browsers can be simple and text based (like Lynx) or very complicated and powerful, like Netscape Navigator or Microsoft Internet Explorer.

URL or **Uniform Resource Locator**: The URL is a descriptor that tells a web browser (or other internet enabled program) where to look for services. One example is "http://www.computerlaw.com." The URL is often used synonymously with the "web address", but in reality it can be used for a variety of protocols, such as "ftp://ftp.microsoft.com" or even a "gopher://" address.

Open Source: The internet was built in part by the sharing of code and "open source." Open source calls for the free distribution of source code, along with free modification of that source code for use by others.[5] Open source went a long way to creating a aura of freedom, sharing, and building on the shoulders of giants. This, of course, creates a problem as the internet shifts to a fee for service model.

E-Commerce: This is discussed in more detail later in this program, but suffice it to say here that e-commerce at its broadest is the conglomeration of transactions, whether personal or business, on the internet. More narrowly, it is the buying of goods and services on the internet.

ASP or **Application Service Provider**: This is a new model of providing services - it is the provision of application or management services over the internet. For

---

[5]A detailed discussion of open source is discussed here: http://www.gnu.org/philosophy/free-software-for-freedom.html

example, Network Associates provides a centralized anti-virus management service through its McAfee ASaP service. Microsoft has begun to offer its Office suite via an ASP - essentially a rental of its software. The benefit of an ASP is that for continuing payments, the latest version of the software is always available for use by the specified number of users.

Instant Messaging and **Chat**: Realtime communications has been available for years through the IRC protocol. However, the text based versions of IRC programs can be cumbersome. America Online popularized chatting by creating graphics based "chat rooms" for its customers. Several companies now offer chat and other conference features (such as shared document editing).

Additionally, "instant messaging" has gained popularity of late. This is a window that pops up on a screen with a message or requesting a chat. This functionality is even available on telephones via the SMS (Small Messaging System) protocol on GSM phones and even through two way radios on Nextel phones. Instant messaging is far more intrusive than electronic mail, because it interrupts whatever the user is doing when a message is received. However, it also provides for a much higher availability for real time discussions.

Streaming: Streaming is a form of data delivery for audio and video. Because audio and video files are large, streaming protocols have been developed that allow for playing of media files before they are completely present on the receiving machine. The result is the ability to watch video or listen to audio as it is being downloaded from a remote location.

IV. Tools of the Trade and Their Operators

The internet doesn't just "happen". Instead, it is built by people and equipment that put it all together. Some of this equipment was discussed above, such as *routers* and *switches*.

Server: A server is a computer – usually a powerful one – that provides whatever shared access the server administrator desires. Servers can provide file sharing, electronic mail relays, world wide web services, or even just computing power. Virtually any computer can be a server, including desktop and laptop computers; this, of course, can lead to security problems.

Intranets and **Extranets**: These are stylized terms that describe "mini-internets" that usually have limited access. An intranet usually refers to a network for employees of a company or members of a group, while an extranet will provide access to clients or customers. These differ from a standard local area network (LAN) in that they provide structured data presentation, typically via a web page.

Client/Server: This model of data processing has gained favor in the past few years. Essentially, part of the processing power is performed at the local computer (the end user's computer) where the display of data is performed, and part of the processing is done at the central server, where the data is located. The benefit is that network traffic is reduced because the data can be processed before it is sent, and processing resources are distributed so that clients (which are less powerful than the server) do not slow down unnecessarily. Common client/server applications are mail programs and high-end databases.

Thin Client: This is a form of computing that hearkens back to the days of mainframe computers and old telnet clients to central computers. The idea is that the computer has just a monitor, network adapter (along with a few other component required to make it work). All other resources, including even the operating system, are located on a central computer, even over the internet. Ostensibly, a person's applications and data would follow them wherever they go, from thin client to thin client.

ISP or **Internet Service Provider**: These are companies that provide internet access to individuals, organizations, and companies. They provide a Point of Presence (or POP) in most cities. The idea is that the "last mile" to the ISP is as short as possible, whether it be through dial-up, broadband, or T1.

Backbone: These are "super-ISP's". They sometimes provide ISP service to end users, but more often they provide internet access to other ISP's.

Peering Agreements: Peering agreements[6] allow backbone providers to connect to each other directly rather than forcing packets to travel through intermediate networks. For example, at MAE's (Metropolitan Access Exchanges) and NAP's (Network Access Points), each network backbone connects to very powerful routers which are all connected to each other. However, there are also fiber optic cables that directly connect two backbones while bypassing the routers.

In short, someone has to pay for access on the internet. User's pay smaller ISP's, smaller ISP's pay larger ISP's, and larger ISP's pay backbone providers. Should

---

[6]An example peering agreement can be found at http://www.ripe.net/ripe/mail-archives/eof-list/19941025-19941201/msg00013.html

backbone providers pay each others? Should ISP's pay each other directly so they don't have to pay backbone providers? Peering agreements help answer these questions - they allow ISP's and backbones to trade access in order to save payments and more efficiently route traffic.

Digital v. **Analog**: Digital data is in the form of 1's and 0's, also known as bits. That is, each bit is either on or off, and the computer will process the series of bits in accordance with how the microprocessor and other computer components are designed. Analog data is sent in the form of high electrical levels, low electrical levels and everything in between - think of a decibel meter measuring all of the volumes as compared to "the clapper" which is either on or off when it hears a sound. Even if data is sent in an analog form (such as through an analog modem), the data is converted to and from digital data for use by computers.

Bandwidth: Bandwidth describes how much network traffic a network can hold. It used to be described a "baud rate" or bits per second – the first modems were 300 baud. Now it is described as kilobits per second or megabits per second. A kilobyte is 1024 bytes. A kilobit is 1024 bits, or roughly 1/8 of a kilobyte (there are 8 bits in a byte). Similarly, a megabit is 1/8 of a megabyte.

People often confuse bandwidth with speed. The two are, however, different. An IP Packet can only travel so fast – the speed of light! The slowdown is when there are collisions among the packets (or more literally, collisions of electrons) in the network. This is why switches are important - they reduce collisions.

Imagine two water pipes. When full, water will travel through the pipes at the

same speed (that is, feet per second) under the same pressure. However, the larger pipe will deliver more water in the same period of time. Bandwidth is the same way - it is the size of the pipe to the internet. For example, if the average amount of traffic for a small office is 256 Kbps, then a 1.5 Mbps connection will never be full, and a 256 Kbps connection would appear just as "fast" as a 1.5 Mbps connection. If, however, a company is transmitting uncompressed video, then even a 100Mbps connection may not be enough to allow all of the data through.

Dial-up and **PPP**: This is internet access via a telephone line and an analog modem. PPP is short for Point to Point Protocol, a protocol used to emulate a TCP/IP network device over a telephone line. The fastest dial-up connections today are no more than 53 Kilobits per second. ISDN modems can provide up to 128 Kbps access, but the use of ISDN has fallen out of favor with the increased speeds of broadband.

Broadband: This is the generic term for a newer form of high speed internet access delivered to homes and businesses. It encompasses DSL (over a telephone line), Cable Modems (delivered with telephone cable), and even a wireless signal (received over long distances from a transmitter). Bandwidth can vary from 184 Kbps to over 5 Mbps.

T1: This is an older form of internet provision (though T1 and T3 lines have been used for point to point networks as well). A T1 is a leased line from a telecom provider (such as the local telephone company). A CSU/DSU is used at each end of the line to convert the signal from IP to a form that can be transmitted over the T1. T1 speeds usually cap at 1.5 Megabits per second. T3's and higher can have significantly higher

bandwidth.

Fiber or **Fiber-optics**: This is the current state of the art in high bandwidth network access. Fiber is a bundle of thin but solid glass cables that carry data signals in the form of light. The bandwidth is extraordinary for a variety of reasons. First, there are almost no collisions. Second, there is far less interference because there is no electro-magnetic movement. Third, data is transmitted digitally (that is, in 1's and 0's) rather than in the form of an analog electro-magnetic wave. Most backbone provides and even many ISP's are using fiber-optics to increase bandwidth on the internet.

Wireless: New standards are available for wireless access either over a short distance or a long distance. Over short distances, the leading protocol is IEEE 802.11b, while a new protocol, called "bluetooth" is being developed. Over long distances, the protocols tend to be more proprietary to the providers, either via ricochet wireless modems, two-way pagers, cellular phones, or handheld PDA devices. Wireless broadband and one and two-way satellite access is also available.

HTML or **HyperText Markup Language**: This is the language is used to define web pages. It consists of a variety of "tags" that define attributes as simple as font size and typestyle, and as complicated as forms, buttons, and graphics. A tag is text in brackets (like for bold). A tag must be opened and closed (such as). The web browser will parse and convert the HTML to the format shown on screen. HTML is a subset of SGML (Standard Generalized Markup Language). SGML generally defines the use of "tags" which are parsed in different ways to create data.

XML or **Extensible Markup Language**: This is a language similar to HTML

because it is also a subset of SGML - it uses tags to data fields and to create a hierarchical set of records. For example, this section might be

<Section><Header>Tools of the Trade and Their Operators</Header>

<Text>The internet doesn't just "happen"....</Text>

<Subsection><Header>Servers</Header>

<Text>A Server is a computer....</Text>

</Subsection>

<Subsection> ...

</Subsection>

</Section>

Aside from being a potential alternate to HTML in web page formatting, XML is viewed today as the panacea of interoperability between different types of databases. The goal is to use XML tags and structures to represent data - if both systems understand the structure, data can be shared.

SOAP (Simple Object Access Protocol): SOAP is an XML based standard that allows for the exchange of information and procedure calls (remote control) in a distributed environment. The goal is to have distributed content and management services so that all data is not compiled in a single location. This is an emerging standard that has yet to be adopted broadly, though it is gaining support.

DOM (Document Object Model): This standard is similar to SOAP - it sets forth the ways that content should be managed and formatted.

Search Engines: A variety of search engines have been created to help manage

the millions of pages of web content on the internet. There are two types of engines. The first are "crawler" type engines, which index all of the words in web pages for retrieval. The better search engines will sort by relevance and popularity. Two of the more popular engines are http://www.google.com and http://www.altavista.com.

The second type are hierarchical search methods. These will select (either by crawling or by submissions) web pages and categorize them by topic. Yahoo, at http://www.yahoo.com is the most popular such site. Few people today know that yahoo actually stands for "yet another hierarchically organized oracle".

Java and **Javascript**: Java is a programming language developed by Sun Microsystems. Its primary distinguishing feature is that it is designed to be computer operating system independent. Any computer that has a Java Virtual Machine on it can run a Java program. The application to the internet is obvious - developers can write one program, and web browser developers can create Java Virtual Machines for each operating system. The result is that the single code will run anywhere.

ActiveX: ActiveX is an interface developed by Microsoft Corporation. Similar to Java, ActiveX controls are executable files that allow for web content providers to provide additional features on web pages. Unlike Java applets, ActiveX only runs on Microsoft Windows based operating systems. However, unlike Java applets, ActiveX can take advantage of a variety of Windows based features.

IT and **IS**: These mean "information technology" or "information services". These are the people who design, manage, and maintain the hardware and software infrastructure that is the internet. They do everything from set up computers to design

software that runs the most powerful web servers and applications in the world (this definition would include software engineers as well).

V. **Data Types**.

There are a variety of data types you will find on the internet:

.htm and **.html**: This is the basic file type for html files - they are rendered to what we see on the screen of web browsers.

.asp and **.jsp**: These stand for active script program and Java script program respectively. These are special dynamic web pages that are built by scripts for either ActiveX or Javascript language.

.avi, **.mpeg**, and **.asf**: These are video file formats, that are played in a variety of media player programs.

.wav: This is the uncompressed audio file format. These files can be enormous - a full three minute song can take 50 or more megabytes.

.mp3: This stands for “mpeg, layer 3”. This is the most popular format for compressing encoded audio files. It’s ability to greatly reduce the size of files has helped fuel a proliferation of music sharing. Despite being smaller than .wav files, these files can take up significant bandwidth and hard disk space if left unchecked. Similarly, companies are growing increasingly concerned with copyright infringement issues by their employees.

.jpg and **.gif**: These are picture file formats. The .gif format is patented, and is not

used often in any event because they are larger than .jpg files due to lack of compression.

.zip, **.gz**, and **.sea**: These are compressed archives - compressing multiple files into a single smaller file was (and is) an efficient way to transfer files across the internet.

.vbs and **.scp**: These are extensions for executable script files – they are the root cause of the proliferation of many viruses. Email programs (such as Microsoft Outlook) can (and used to automatically) execute scripts attached to incoming electronic mail. The script would then send itself to the people in the user's electronic address book.

VI. Issues for the Future.

The "New" Communications. Electronic mail, chat, and instant messaging has forever changed the way people communicate. How will this affect personal relationships? What effect will this have on dispute resolution? Will communications evolve even further? Indeed, Microsoft's new "Hailstorm" initiative is a set of instant messaging building blocks for developing applications. In this view of the world, all communications are instant!

Battling Standards: An issue now and in the future will be the battle for standards. New standards battle for desktop supremacy every day, such as ActiveX and Java. Of course, we might prefer that the "best" or most "efficient" standard win out, but such is not always the case.

Encryption: Encryption is the process used to convert "clear" or "plain" data into a form that cannot be read without the encryptor's consent. Secured Socket Layer, or SSL, is a form of encryption used to allow web browsers to communicate with web

servers in an encrypted manner.

Terms of Service or **TOS**: Companies offering web services will frequently provide a terms of service agreement. This is a typically unsigned and even unseen (though some providers require users to "assent" by clicking a button) document that describes the rights and responsibilities of both the web user and the web content provider.

Privacy: A primary concern for web users is the privacy of their data. The concern can be as mundane as associating web sites visited with an email address (hence causing spam) to theft of credit card numbers. Many web content providers have privacy policies as part of their terms of service. Others will use SSL and other encryption to protect data. Still others will sell data to mass marketing companies without hesitation or shame. Some will do all three at once.

Spam: Spam is the term often used for unsolicited commercial electronic mail. At its broadest, it includes any email sent to a user without the consent of the recipient. Organizations such as Mail Abuse Prevention System LLC (MAPS) at http://www.mail-abuse.org have tools to fight spam.[7]

Virus: A virus is a computer program that gets installed on a computer either by forced entry or accidental installation. Viruses can be as benign as popping a message up for the user to read, to as malicious as destroying a hard disk or even a hard disk on a network server. Some viruses will self propagate by reading the email address book of

---

[7]Russo & Hale LLP has represented MAPS.

the user and sending itself to other people. The "I Love You" and "Melissa" viruses were two examples of this type of virus. The two most popular anti-virus programs on the market are Network Associates' McAfee VirusScan and Symantec's Norton Anti-virus. It is important that these programs be updated frequently, as viruses change over time and new ones are invented regularly.

Trojan Horse: A trojan horse is a special kind of virus. This program either mimics an actual program or simply installs itself in a hidden place while giving access to others. One well known trojan horse is "Back Orifice" which basically allows others full and complete access to the computer.

Copying: Despite the 9th Circuit's decision in Napster,[8] the state of allowable copying on the internet is not clear at all. The extent to which files can be shared and by whom will be a subject of debate for years to come.

Hackers and **Crackers**: In the old days, people who "hacked" or intruded in to computer systems were all called hackers. Those who did so for fun, or for purposes of good (ignoring of course the wrongfulness of the breaking act itself) were apparently not happy being categorized with those who intruded for impure reasons. Thus, the term "crackers" was born. Crackers are essentially hackers in the evil universe, and they are the ones who unleash viruses and steal credit card information. Hackers prefer to expose weaknesses of computer systems and then tell the world about it in an effort to get the problems fixed.

---

[8] Napster, Inc. v. A & M Records, Inc., Nos. 00-16401 and 00-16403, slip op. (9th Cir. Feb. 12, 2001).

VII. Introduction to Legal Issues

By now, you should have an idea of some of the legal issues that may arise relating to the internet. Here are few questions to ask yourself as we proceed:

- Should the ".com" be given any weight for trademarks?
- How do domain name disputes change when a registered trademark is involved?
- Can the internet help invalidate patents?
- Is the internet creating too many business method patents?
- How can anything be trade secret on the internet?
- How has the history of sharing on the internet changed they way we look at copyright in cyberspace?
- Where can a court exert jurisdiction with a web server in one state and the parties in different states?
- Can someone be defamed in email? What about a usenet group? Where is the jurisdiction?
- Are online contracts valid? What if the user never even saw a terms of service document?
- What kinds of privacy expectations should attorneys and clients have on the internet?
- Can we or should we punish hackers for trespass? What about other web sites that copy information from our own?
- Should we allow email providers to block spam? Is there tort or contractual liability if they do?

- What kind of security should e-commerce providers have? Should they be forced to offer this security?
- Are there product liability issues for bugs in web site design and operation?

The internet is the source of these questions, and more. Understanding how the internet works is vital to examining how to go about answering these questions.