Payoff

Laws pertaining to the Internet are emerging as the system matures. Large end-user organizations are discovering the true nature of technology’s influence on business relationships. This article discusses the critical areas of the law and legal liabilities for organizations doing business over the Internet, and uses examples of recent cases to demonstrate possible outcomes of legal action.

Introduction

The legal environment of the Internet has often been compared with the Wild West in the days of the American frontier. This analogy is used to convey the wide open and freewheeling atmosphere that pervades this area of the law. The Internet, like many other technological phenomena, is developing along several parallel directions. The main line is the technology direction—those facets of networking, computing, software, and data base, which, when combined, add up to the ability to access the array of interconnected computers known as the Internet.

The second area of development is the nature of business on the Internet. How can information be exchanged? How can goods or services be bought or sold? What aspects of today’s business rules can be effectively employed as rules for tomorrow’s net-based business?

It is only after business transactions are in process or, more properly, when business transactions do not turn out according to the expectations of the participants that the law enters into the picture. Astute managers do not resort to the law to correct a problem; rather, the law is supposed to be used as a guideline to avoid problems or to minimize the consequences if things go wrong.

Therefore, it follows that the law of the Internet is an emerging and evolving beast. Large end-user organizations are turning to technology first and then are immersed in the process of figuring out how to use that technology. Once the technology is employed, the true nature of its influence on business relationships can be determined. The deeper and more mission-critical the use of technology is, the more severe the effects are if something goes awry. When it is clear that a simple business solution will not work to resolve a problem, lawyers are called.

Defining the Situation

To understand the sheer magnitude of the dilemma of law on the Internet, it is useful to look at the Internet through an analogy. John Anderson, the former Presidential candidate, speaking at the annual RSA Conference in Redwood City, California in January 1995, compared the Internet with interstate highways. He pointed out how, back in 1955, no one could have foreseen the economic fallout of the interstate highway network. Originally set up during the Eisenhower administration as a key part of its Civil Defense strategy, the interstate highway network spawned not only a multibillion dollar auto and truck industry, but had a profound effect on shipping and on population concentration. No one could have looked at the way highways would either spur or destroy commerce and communities.

At present, the Internet and its subsequent progeny are similarly unknown and unpredictable. From a legal perspective, this situation becomes particularly perplexing. When stripped to its core, the purpose of a legal system is to form a bulwark upon which a
set of governing behaviors can be determined. The split of law into civil and criminal areas has historically been used to divide the legal world into two segments: a part that deals with interaction among parties (i.e., civil law) and a part that governs an individual's (or organization's) behavior with respect to society (i.e., criminal law).

From a US perspective, civil law may be further divided into multiple areas: areas of legal specialty and jurisdictions. As law relates to the Internet, areas of consequence are:

- Contract law.
- Intellectual property.
- Torts and negligence.
- Criminal law.

Before addressing each one of these areas in turn, it is important to point out that laws are not enforced in a vacuum. A critical aspect of the law is jurisdiction. Jurisdiction has two dimensions: the party and the law. The first jurisdictional issue is: does the court have the power to control an individual or entity? In the United States, a court's jurisdiction may be a city, county, state, several states, or the entire country.

The second question is one of subject matter or rules. Plaintiffs (i.e., the parties bringing a suit) determine where they will bring the action; that is the legal forum. If the plaintiffs and defendants (i.e., those charged by the action) are from different locations and if the matter at hand occurred in yet another location, various procedures are set in motion by both sides to decide which set of rules (i.e., body of law) will be applied by the court. This is especially true in a federal court that, although located in one state, will often be compelled to follow the law of another. This jurisdictional issue is called diversity of citizenship, whereby the law of one state may be applied to adjudicate a dispute in a court of another state.

There is no greater challenge to jurisdiction than that of an indefinable web of computers and the various media that link them. The Internet is conceptually stateless and countryless, so jurisdictional issues are wide open. Some of the key aspects of litigation, such as forum shopping (i.e., picking the best place to bring the action), is discussed in a later section. Moreover, courts need two kinds of jurisdiction to try a case: personal jurisdiction over the parties and subject matter jurisdiction over the matter. One is not enough; both are necessary.

The next sections highlight significant areas of the law and how they relate to the Internet and its security and integrity.

**Contract Law**

The Internet may become not only a transportation medium for business transactions, but the subject matter as well. Existing rules of law and terms and conditions that govern business transactions, such as the Uniform Commercial Code, must be modified to bend to the Internet way of doing business.

A number of reforms have been under way for several years on different fronts. A key area of contract law that is evolving is EDI. Organizations can employ EDI to replace paper transactions. If so, clear terms and conditions must be extended to encompass new concepts of contractual relationships. Key terms, such as acceptance, rejection, and remedies for breach of contract, must be couched in terms appropriate for the Internet world. Potential failures or compromises of Internet-based transactions, failure to perform by Internet service providers, as well as action or inaction by suppliers and customers must be considered in developing contracts between organizations using EDI.
Areas of particular interest to Internet security practitioners include the use and acceptance of digital signatures in lieu of written signatures. A digital signature is the use of an algorithm as a substitute for an individual's authorized, holographic signature. The purpose of the signature is to commit the signer. It is an authentication of the signer's intent and proof of his or her acceptance or authoring of the document at hand.

The main reason behind the push for digital signatures is the UCC. Used by 49 states (the exception is Louisiana), the UCC requires both parties to sign a writing for transactions in excess of $500. As a side note, there are other branches of the law, such as real estate, where a signed writing is also required for the transaction to be valid. Digital signatures could be employed in a number of other areas in which the legitimization of documents is important.

**Intellectual Property**

Intellectual property is made up of several key components: patents, trademarks, copyrights, and trade secrets. For the most part, intellectual property is a part of state craft; that is, federal law controls its validity and use. Only trade secrets are governed by state law. From the perspective of the Internet security practitioner, a fair number of rules are already in place. Violations or, more commonly, infringement of intellectual property rights can occur throughout large end-user organizations. The availability and convenience of E-mail and the Internet as a transportation medium increase the reach of a potential infringer. The literally unlimited horizons of the Internet raise the stakes for intellectual property problems.

The astute practitioner will bolster him or herself through aggressive policies and extensive education. Employees and others with access to an organization's intellectual property should be placed under contractual control not to use that property improperly. As with other aspects of employee-related legal issues, notice and consent are critical. Organizations must be obligors on notice as to what information is a trade secret, and they must place conspicuous notice on copyright or trademarked items.

Organizations must remember that the Internet is another way in which employees can transport protected property to unauthorized parties. They must guard against the possibility of this occurring as they would with more traditional vulnerabilities.

**Torts and Negligence**

In cases involving the Internet and in others involving negligence, courts will apply (and will instruct jurors to apply) classic test factors. The common law test applied in these situations has the following elements:

- **Gravity of the harm**: how extensive was the damage?
- **Likelihood to occur**: given the surrounding circumstances, how likely was the event to happen?
- **Cost to prevent**: Given the size of the potential harm and its likelihood, what would have the cost been to prevent the harm and how reasonable would it have been to expend those funds?
- **Duty of care**: What responsibility did the defendant have to the plaintiff? For example, because banks hold their depositors' money and are considered fiduciaries, they are held to a higher standard of care than a simple vendor of stationery goods would be.
Standard of care: What do other similar persons or organizations do under the same circumstances? Do 95% or more of similar victims of a crime perpetuated over the Internet employ firewalls? How sophisticated is the victim as an Internet user or provider?

These factors will continue to be the yardsticks by which negligence actions will be measured.

Product liability is an area within tort law in which products used in Internet applications are included. By way of analogy, the New Jersey Supreme Court in Roberts v. Rich Foods, Inc., 139 N.J. 365 (1995) found that a computer used in a motor vehicle was defective. This computer was used by truck drivers to record mileage and fuel data. The court judged it as defective, because the device could be operated while the vehicle was in motion. It was reasoned that operating the computer would divert the driver's attention from operating the vehicle, so that if there was an accident, the design of the computer would be a factor in that accident, and liability of the computer manufacturer for improper design had to be considered.

Criminal Law

Criminal law is a creature of the government. The plaintiff is the government or “The People.” To be guilty of a crime, one must have “broken the law” or violated a particular statute. Typical criminal law statutes require a voluntary or involuntary action (i.e., actus reus) in legal jargon and an intent (i.e., mens rea). Usually, Internet and other computer crime laws require voluntary acts (as opposed to involuntary or unconscious acts) and purposeful intent. Therefore, government prosecutors must be able to prove both. This proof must be to the higher standard known as “beyond a reasonable doubt,” which contrasts with civil law, where the standard is preponderance (i.e., majority) of the evidence.

Often, as with other laws, computer crime laws are shaped out of well-known past rules. For example, criminal harassment activity, stalking, and similar behavior have been a part of the legal landscape for some time. In June 1995, the State of Connecticut joined the ranks of computer crime pioneers by amending its existing harassment law to include a “computer network” as a means by which a defendant could employ with “the intent to harass, annoy, alarm, or terrorize.” Details can be found in the Connecticut General Statutes, sections 53A to 182b, and 183.

Another important aspect of Internet criminal law that is currently being addressed is the issue of sentencing guidelines. Sentencing guidelines are issued by various jurisdictions and are used by judges in dealing with the post-trial punishment of defendants who have been found guilty. Among the aspects of sentencing guidelines is “sexual abuse or exploitation.” (For reference, look at the United States Sentencing Guidelines, section 2G2.2[b][4].) The First Circuit Court, based in Boston, MA, felt that the transmission of child pornography over the Internet (in this case, America Online, or AOL) did not constitute sexual abuse or exploitation under the guidelines. The case in question was United States v. Chapman, 60F.3d 894 (1st Cir. 1995).

In this case, according to the court, there was “considerable evidence” that the defendant used AOL to transmit child pornography on a number of occasions. The court concluded that these transmissions were not abuse or exploitation under the guidelines; therefore, these transmissions should not be considered a factor in deciding an appropriate sentence.

The Computer Fraud and Abuse Act of 1986 serves to protect computer systems, particularly federal computers. United States Code Section 1030 (a)(5)(A) states that its penalty provisions apply to “anyone who intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct, alters,
damages, or destroys information in any such Federal interest computer or prevents authorized use of any such computer or information...” and thereby causes loss of $1,000 or more.

It is important to note that the term “Federal interest computer” broadens the scope of the law to more than just federal government computers. It would logically include contractors to the federal government and perhaps computers privately owned by US federal government employees that are being used for the benefit of the federal government. It is also interesting to note that loss of use receives protection under the statute as well as damage or alteration.

The most well-known conviction under this statute, upheld on appeal, was the case of the Cornell graduate student, Robert Morris (son of the NSA cryptographer), who was convicted for releasing the “worm,” a computer virus that replicated itself over the Internet, causing multiple crashes. Among those computers affected were a significant number of “Federal interest computers.” The appeals court's opinion may be read at United States v. Morris, 928 F.2d 504 (2d Cir.), certiorari denied by the Supreme Court in 502 US 817 (1991).

**Export Control and International Traffic in Arms Regulations (22 CFR, Parts 120 through 128 & 130)**

These regulations are used to control export of anything that could harm the security of the United States. This includes weapons, weapons systems, and cryptography. Vendors seeking to export must secure an export license. The approval process weaves a circuitous route among the Departments of Commerce, Defense, and State. Although the process has been a thorn in the side of US software exporters, it has spawned a specialized consulting niche. This niche has been addressed by a number of independents, most recently by RSA Data Security, in Redwood City, CA. RSA recently announced a new division in the company, which will be headed by a former employee of the National Security Agency (NSA), to assist companies in obtaining export licenses. There are also a number of independent consultants, such as Cecil Shure, president of CSI Associates, in Washington, DC, who specialize in exporting.

In fairness, the Clinton administration has been sending a number of signals that it is willing to relax the draconian regulations under certain circumstances. Among these, are the vendor's willingness to give the government access to key-breaking information when the government asks for it, or as a part of the approval cycle. This is both good news and bad news for vendors. On the positive side, the approval process may, at last, be getting more export friendly. On the negative, non-US customers may not be willing to employ a product knowing that the US government is able to “read their mail.”

**Liability Issues**

Anyone can be named in a lawsuit or charged with a crime. The “who” can be an individual or an organization. Ancillary potential plaintiffs and defendants in Internet matters can include suppliers, customers, government agencies, and trade associations, to name a few possible candidates.

**An International Perspective**

In an unusually frank spirit of cooperation, the forum for suit was broadened in Europe to allow defamation plaintiffs domiciled in a Brussels Convention country to pursue remedies either where the publication originated or where the harm occurred. The choice of litigation could therefore be based on a greater likelihood of success under that country's laws or the reputation for plaintiff sympathy. (Plaintiffs choose where to bring actions;
defendants merely respond.) Reference for the European Court of Justice is C-68.93 and the United Kingdom (UK) reference is Shevill v. Presse Alliance CA (1992) All ER. The defendant was a French publisher, and the action was brought in the UK because the plaintiff felt that the UK was a more sympathetic jurisdiction. The court noted that circulation was greater in France than in the UK, but that was not material to the selection of forums.

A Role in the Events

In general, a party cannot be found liable unless it had some part in the problematic acts. For purposes of the law, the party can just as easily be an organization (government or private) as well as an individual. Of particular interest to the Internet community is the issue of publisher liability. One who creates or edits the “news” is far more likely to be found culpable if there is a liability issue than one who merely distributes or transmits the news.

A New York case, Stratton Oakmont Inc. v. Prodigy Services Co., No. 31063/94, 1995 WL 323710, 23 Media Law report 1794 (N.Y. Supreme Court 1995), was decided against the on-line service. The facts involved comments posted by an unidentified bulletin board user in October 1994. These comments on “Money Talk” contained allegedly libelous statements about Statton, an investment banking firm. Stratton sued both the poster and Prodigy.

The rationale behind this decision covered a number of relevant points. Prodigy employed moderators for the panels. These “Board Leaders” had a number of responsibilities over the bulletin board. These leaders were charged with enforcing the content guidelines set up by Prodigy (the guidelines themselves were considered another reason why Prodigy had control over content) and could use a special delete function to remove offending material. The court also noted that Prodigy employed software to screen postings for offensive language. Another critical aspect of this case was that the Board Leader of Money Talk was found to be an agent of Prodigy and that agent liability attached.

The opposite ruling (that is, finding that the service provider was not a publisher) was the 1991 case in the Southern District of New York, Cubby Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991). In this case, the court felt that CompuServe did not post any guidelines, take any role in controlling content, or promote itself as a family-oriented service, as Prodigy had.

Organizations can be found liable for the actions of their employees or agents under the legal doctrine of respondeat superior. Simply stated, employers can be liable for the acts of their employees acting within the scope of their employment. Therefore, software developers who accidentally unleash a virus or worm, as Morris did, may bring liability upon their employers. In addition, plaintiffs will continue to search for defendants with money. Often employers have more financial wherewithal than their employees and become the targets of legal action.

Some areas of the law look to what management actually knew or should have known given “due diligence” of the reasonable person under similar circumstances. Intentional acts by employees that can or should have been prevented by more direct action by management may also result in liability applying to the organization, even for intentional acts.

Another rule of law, which is that intentional criminal acts are a bar to liability, may also be applied in Internet security cases; however, there are no guarantees. Juries have often gone against facts that appear to be overwhelming and appellate jurisdictions have often labored to reach a decision based on abstract theories of society goodness. The absence of historical precedent makes legal actions by and about the Internet perfectly positioned for inconsistent decisions. Security practitioners who go down this uncharted road do so at their peril.
Product Liability

Anyone in the “stream of commerce” can be included as a party in a product liability matter. Included in the stream of commerce are designers, developers, manufacturers, distributors, representatives, and retailers. An aggressive plaintiff and competent counsel will seek to embroil any potential defendant in litigation. This is especially true if the defendant has significant financial resources or a track record of trying to settle rather than litigate matters. This will undoubtedly be an important aspect of future Internet legal activity.

Liabilities and Available Remedies

The ultimate purpose of remedies is to put the aggrieved party back into the position that he or she would have been in if the wrongdoer had not acted in the way that he or she did. Remedies can also be used to deter future negative behavior and compensate the plaintiff for wrongs against society committed by the defendant.

Money Damages

A court can award substantial sums of money to the aggrieved parties. Their rationale can be real or imagined. Amounts can be rational or irrational. Experts are often used to “prove up” damages. The role of the expert witness is to clarify facts for the court. As shown in a recent, celebrated criminal trial in Los Angeles, scientific, expert testimony does not necessarily ensure victory for the presenter. In addition to damages as a result of the defendant's act or failure to act, damages can be awarded based on a “bad intent” on the part of the offender. These punitive damages can often be twice or three times the amount of actual damages.

Injunctions

An injunction is simply a court order prohibiting a party (or parties) from doing a specific action. To get an injunction during the pre-trial phase, plaintiffs have to demonstrate (among other things) that they will suffer irreparable harm if the injunction is not invoked, that the plaintiff is likely to win on the merits of the case (which will result in a permanent court ruling), and that the court will be able to enforce the injunction.

Criminal Liability

Remedies in criminal cases are spelled out by the statute that was violated and the sentencing guidelines that jurisdictions often issue to accompany the laws. The most common punishments include fines, community service, and incarceration. Incarceration can take many forms: county, state, or federal prisons; and a growing number of other more innovative programs such as confinement to one's home.

Courts have sometimes gone to great lengths in computer-related crimes to remove a convicted defendant's access to the tools of the computer trade. The incorrigible nature of some defendants and the magnitude of the harm they caused, combined with their lack of remorse, have often induced judges to impose heavier and more creative sentences than in comparable cases of non-computer-related crimes.

Lawyer Liability

Lawyer liability is a phrase that the author uses to describe other harm. Time spent with and money spent on attorney's fees are not trivial. In the days of downsizing and
rightsizing, employee productivity is zealously guarded. Time spent that does not either increase revenue or decrease costs is wasted time. The effort and resources needed to pursue and win a legal action should be considered before the action is undertaken. Fees for attorneys, as well as other expenses, such as court costs and expert fees, are substantial. Often plaintiffs have to spend an inordinate amount of time educating their counsel about the nature of their businesses and the nature of this action. Combine this time investment with the uncertain nature of law as related to the Internet and the general lack of computer literacy in the legal profession and there are the makings of a true disaster in terms of the expenditure of resources versus the likelihood of benefit or gain.

This approach could be applied to computers as well. Given the seemingly pro-right wing and pro-conservative American electorate and the noncommittal nature of leading politicians and their desire to win the family vote, a strong push to repeal such infringements is not likely to come from elected officials. Rather, it will be up to pioneering plaintiffs, perhaps aided by the Electronic Freedom Foundation (EFF) or Computer Professionals for Social Responsibility (CPSR) or other similar rights advocates to step up to employ legal action to block enforcement.

Such activity is not unprecedented. The California proposition 187 limiting educational and other entitlements of immigrants, which, although passed by the electorate, was blocked due to potential constitutionality problems, could be a model for such protestations. However, computer and information freedom does not have a readily identifiable homogenous group of affected persons who will take direct, immediate, and costly action, at least not at this time. Furthermore, championing of pornography is not a popular view that will capture the hearts and minds of the electorate or the media.

### Avoiding Problems

System administrators must be mindful of the need for notice and disclosure. They must ensure that users or subscribers are fully aware of who has access to the system. They must indicate clearly how monitoring and control may be or is exercised on the system. Employee handbooks should spell out exactly what employees are expected to do in terms of use of the company’s information resources. All employees should sign an acknowledgement that they have read the rules, understand them, and agree to be bound by them.

### Prosecution of Hackers

It is important to remember that a criminal prosecution is run by the office of the local District Attorney (DA), not by the victim. The goal of the DA is to get a conviction, not to ensure that the victim is compensated; nor is his or her goal to prevent similar occurrences in the future. A decision to proceed with prosecution is also a decision to cooperate fully with law enforcement authorities. Cooperation may require a significant amount of time, money, and resources from the company. This commitment may not fit with the company’s goals of minimizing bad publicity, fixing the leak, and controlling the course of legal events.

Should the decision be made to proceed, it is important to be mindful of the rules of evidence and the critical need to keep a pure chain of custody. One person's opinion that a piece of evidence is damning does not mean that it is and, more importantly, it does not mean that it will be admissible and, if it is, that it will be understood by the trier of fact, whether judge or jury.

It is important to recognize that experts may be needed and that they may come from the ranks of the company or the company’s suppliers. Victims may not be in a position either to recommend, to supply, or to compensate needed experts, and the District Attorney's budget may not permit hiring the “right” kind of talent.
History has shown that a defendant with financial muscle is not to be taken lightly. Should the defendant be well funded, he or she might not get convicted, and might turn around and sue the plaintiff for defamation or malicious prosecution.

Before opting for a criminal prosecution, a lot of good information can be found in a Government Printing Office document: the Criminal Justice Resource Manual, prepared by the Department of Justice. It contains good advice concerning the types of computer crimes, evidence, likely perpetrators, and other related material.

Companies contemplating this type of prosecution should also be sensitive to the track record of the local DA with respect to this type of white-collar crime case. Obviously, some jurisdictions (such as Austin, TX; Boston, MA; and Santa Clara, CA) are better venues for technology-related cases due to the high population of computer literate potential jurors and high-tech companies.

It is critical to remember that when the lawyer is called, whether a civil counsel, corporate counsel, or the local DA, someone loses time, resources, and money.

Conclusion

An organization should determine its goals early on in the process and balance the practical results that it wants to achieve against the legal hurdles that will have to be navigated to get them. Often, compromise is a faster, cheaper, and better alternative than pursuing legal remedies. Simple themes are always better than complex ones.

Author Biographies

Lawrence D. Dietz

Lawrence D. Dietz, Esquire, is vice president of Knowledge Centers at the Giga Information Group in Santa Clara, California.