United States

Seth M Reiss[1]
Lex-IP.com
Honolulu, Hawai`i, United States

Overview of the Legal and Regulatory Framework

The regulation of public digital networks and e-commerce in the United States is accomplished through the interplay of federal and state constitutional, statutory, regulatory and common laws. At the federal (centralized) level, there is statutory law circumscribed by federal constitutional mandates. At the state (decentralized) level, there is statutory and common law circumscribed by both federal and state constitutional mandates.

Whereas federal law governs activities within the 50 United States and a handful of United States territories, with some purporting to have limited extraterritorial reach, state law governs each of the individual states (also with some purporting to regulate conduct beyond their borders). Analogous in some respects to the interrelationship of the centralized and decentralized regulatory regimes currently found among member states of the European Union (EU), the framework regulating digital networks and e-commerce in the United States requires an examination of a hierarchy of laws and an analysis of which laws govern the particular activities at issue.

When Congress enacts federal legislation, inconsistent state laws are preempted. Congress also may reserve an area unto itself though fail to regulate the topic. On the other hand, if Congress legislates in an area prohibited by the United States Constitution, such as subject matter the United States Constitution regards as reserved for the states, or if Congress legislates in a manner contrary to a constitutionally protected right, such as laws having a tendency to suppress free speech, courts may strike the law as unconstitutional.

In areas in which Congress has not legislated, or where Congress has legislated in a way to permit states to regulate concurrently, the states are free to legislate. If a state legislates in a manner prohibited by the United States Constitution, or prohibited by the constitution of that state, or where a state legislates in manners that conflict with federal law or in any area which Congress has by indication reserved unto itself, courts may strike down the law as unconstitutional or preempted. Similarly, state common law, being the

[1] The author wishes to acknowledge the invaluable assistance provided by Brandon U. Davidson, of Watanabe, Ing & Komeiji, LLP, and Bryan M. Harada, of Godbey Griffiths Reiss, LLP, in updating this chapter.

law arising from case precedent, will be declared unconstitutional and ineffectual if it attempts to regulate in an area or manner incompatible with the federal or state constitutions or an area preempted by Congress.

Article I, section 8, of the United States Constitution endows Congress with the exclusive authority to legislate matters affecting commerce among the 50 states of the United States and foreign commerce. To the extent Congress fails to regulate interstate or foreign commerce, an implied constitutional limitation on state power, referred to as 'the dormant commerce clause,' precludes states from enacting laws which discriminate or unduly burden interstate or foreign commerce.[2]

Congress' authority to regulate interstate and international commerce includes activities that cross state and national boundaries as well as activities that occur wholly within one state but which can be expected to have a significant economic impact upon another state or country. Accordingly, the regulation of digital networks that use any aspect of a public communications network would necessarily be within Congress' authority to legislate.

Similarly, anything sent or received on the public Internet, and therefore all aspects of e-commerce, are within Congress' authority to legislate. And while states also are at liberty to regulate public digital networks and e-commerce that are present or that take place within their respective borders, states may only do so if such regulations are not inconsistent with federal laws and regulations, do not attempt to regulate an area which Congress specifically reserved unto itself, are not discriminatory and do not unduly burden interstate or international commerce.

Provincial governments are at liberty to legislate in areas not regulated or otherwise preempted by federal and state governments. Most provincial regulations pertain to purely local matters such as land use. Therefore, apart from those land use regulations that concern themselves with the installation of telecom landlines and radio transmitters, for example, provincial regulations do not play a role in the regulation of public digital networks and e-commerce in the United States

It is not possible in the context of this work to comprehensively describe and intelligently discuss all the constitutional, statutory and regulatory provisions and common law doctrines that regulate, directly and indirectly, the Internet and e-commerce in the United States. What is presented below is a survey of United States law and policy regulating the Internet and limited analysis and discussion of that law and policy. The survey does not, for the most part, attempt to address the federal, state and local laws and rules that regulate the providers of the Internet infrastructure -- the telecom, wireless and cable companies. The laws that are discussed are discussed in summary form, with considerable details left out.

Much more has been written on this topic. The legal analysis of any specific e-commerce problem or case may require consideration of laws that are not mentioned or laws mentioned but not fully discussed below, and will almost inevitably require attention to details not includable in a survey of this nature. Accordingly, this survey should be viewed as an introduction to the laws, regulations, and policies discussed, and not as a compre-

[2] *City of Philadelphia v New Jersey*, 437 US 617 (1978).

hensive or final statement on any such laws and regulations, nor as a tool with which to perform an exhaustive legal analysis.

Intellectual Property Issues

In General

The ease with which materials can be appropriated, misappropriated, disseminated, and published on the Internet generates opportunities for the misuse of intellectual property and challenges for the intellectual property owners.

Intellectual property falls into four protected classes in the United States, as it does in most countries: copyright, trade mark, patent and trade secret. All but patent protection are implicated by content placed upon and transmitted through public digital networks. Patent protection is implicated by software used in and business methods practiced on the Internet.

Copyright

Copyright, a matter of federal law, is defined to protect most 'original works of authorship fixed in a tangible medium of expression' and includes original literature, music, drama, choreographic works, pictorial, graphic and sculptural works, audiovisual works, sound recordings and architectural works.[3] Computer programs and graphical user interfaces both qualify for copyright protection. Where a graphical user interface embodies a method of operation, however, the functional aspects of the interface, although embodying design elements, may be ineligible for copyright protection.[4]

The quantum of originality required to qualify a work in the United States for copyright protection is very modest.[5] Since 1989, when the United States joined the Berne Convention, formalities, such as copyright notice and registration, are no longer a prerequisite to a claim of copyright.

Copyright law protects against the reproduction, distribution (including sale), display, performance, and transmission of protected works and preparation of derivative works, without the consent of the copyright owner.[6] The copyright owner is the author except where the work is created by an employee within the scope of employment or under a written signed work for hire agreement or agreement conveying copyright ownership.[7] The current copyright term begins upon the work's creation and continues for the author's life plus an additional 70 years.[8]

---

[3] 17 United States Code, s 102(a).
[4] *Lotus Development Corp v Borland International, Inc*, 49 F.3d 807 (1st Cir, 1995), aff'd, 516 US 233 (1996).
[5] *Feist Publications, Inc v Rural Telephone Service Co,* 449 US 340 (1991).
[6] 17 United States Code, s 106.
[7] 17 United States Code, 201(b); *Community for Creative Non-Violence v Reid,* 490 US 730 (1989).
[8] 17 United States Code, s 302.

In *Playboy Enterprises v Frena*,[9] a district court clarified that the posting of a copyright protected image on a publicly accessible electronic bulletin board without permission of the copyright owner infringed upon the copyright owner's distribution right. In *Sega Enterprises Ltdv Maphia*,[10] another federal district court confirmed that the uploading of copyright protected material to an electronic bulletin board constituted the making of unauthorized copies of the work. One who has a single user license to a protected, subscription based website and shares his or her username and password with others for the purpose of allowing them to also access the copyright protected materials on the website may be liable for copyright infringement.[11]

Those who do not infringe directly but, instead, encourage, facilitate or benefit from third-party copyright infringement can find themselves liable for infringement vicariously. In *A & M Records, Inc v Napster*,[12] a federal court of appeals found Napster, the operator of a peer-to-peer music exchange system, liable for contributory copyright infringement even though the operator only provided the software and maintained the centralized index used by unrelated third parties to swap pirated music. Napster did not itself engage in any duplication or transmission of the bootlegged music. Later, in *MGM Studios Inc v Grokster, Ltd*,[13] the United States Supreme Court went a step further to rule that Grokster, which merely promoted a pure peer-to-peer music exchange system that functioned solely between swappers without the need for a centralized index, was vicariously liable by virtue of having promoted the system for its commercial benefit.

Investors in Napster are being pursued by the record labels for secondary liability for inducing copyright infringement through their funding of the Napster business model. Conversely, third party payment processors were held not liable for secondary liability due to processing payments associated with websites that illegally display copyrighted works because they neither induced nor materially contributed to the web publisher's infringing activity.[14]

Not all copying, display, and dissemination of copyrighted works constitute copyright infringement. Limited non-commercial use of a copyrighted work, even without authorization, may be protected by the free speech guarantee found in the First Amendment of the United States Constitution or the 'fair use' privilege codified in the Copyright Act.[15] Thus, for example, in *Kelly v Arriba Soft Corp*,[16] a federal court of appeals found that the use of 'thumbnail' versions of web pages incorporated into search engine results was protected as fair use and did not infringe, whereas displaying the full-sized images after the user clicked on the thumbnail image did not qualify as a fair use but rather infringed upon the display right of those owning the copyright in the reproduced web pages.

---

[9] *Playboy Enterprises v Frena,* 839 F Supp 1552 (MD Fla, 1993).
[10] *Sega Enterprises Ltd v Maphia*, 857 F Supp. 679 (ND Cal, 1994).
[11] *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991 (E.D. Cal. 2007).
[12] *A & M Records, Inc v Napster*, 239 F.3d 1004 (9th Cir, 2001).
[13] *MGM Studios Inc v Grokster, Ltd,* 125 S Ct 2764, 162 L Ed 2d 781 (2005).
[14] *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n,* 494 F.3d 788 (9th Cir. 2007)
[15] 17 United States Code, s 107.
[16] *Kelly v Arriba Soft Corp,* 280 F.3d 934 (9th Cir, 2002), followed recently in *Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).*

The Digital Millennium Copyright Act, enacted in 1998, implements the World Intellectual Property Organization (WIPO) Copyright Treaty and WIPO Performances and Phonograms Treaty. Title I of the Digital Millennium Copyright Act prohibits circumvention of technological measures designed to control access to copyright protected works as well as the importation and trafficking of devices designed to facilitate the circumvention of such technological measures. Title I also prohibits providing false copyright management information and the removing of copyright management information. Copyright management information would include the title or author of a work, and the notice of claim of copyright.

Title II of the Digital Millennium Copyright Act protects ISPs and other Internet intermediaries from claims of copyright infringement for conduct normally consequent to their provision of services, as for example reproduction and storage of content consequent to caching, and storage of copyright protected material at the direction of a system user.

Every graphic, photograph, video clip, music bite, section of text, and website design, posted on, uploaded, downloaded, or otherwise transmitted via the Internet implicates copyrights and the exclusive rights granted to the owners thereof. All Internet content must be evaluated in terms of whether a claim of copyright in the work may subsist and, if so, whether rights in the work may be taken or whether a privilege or other defense to infringement resulting from the posting or transmission of the content may be available.

Trade Marks and Unfair Competition

Trade mark and unfair competition law protects against the misappropriation of a mark or designation of source or origin of the goods and services of another, and also against the confusion or deception that can result when a junior user adopts a mark or designation that is likely to be confused with a mark or designation already in use by a senior user. Trade marks and unfair competition are regulated in the United States by the Lanham Act[17] at the federal level and by both statutory and common law at the state level.

Unlike the laws of most other countries that protect the first to file a trade mark claim, the first to adopt and use a mark within a given territory in the United States accrues common law trade mark rights in the territory in which the mark is used, even in the absence of registration. State registration of a mark generally entitles the trade mark holder to exclude others from later adopting the same or confusingly similar mark within that state, whereas a federal registration will entitle the registrant to exclude others from later adopting the same or confusingly similar mark anywhere in the United States.

In the case of a pre-existing common law user, one who later registers the same or similar mark will be entitled to prevent the common law user from expanding its use of its mark, but the registrant will not be entitled to use the registered mark in that territory in which the common law user accrued pre-registration rights.[18]

---

[17] 15 United States Code, ss 1051 *et seq.*

[18] *Burger King of Florida, Inc v Hoots*, 403 F.2d 904 (7th Cu, 1968).

Use of the same or similar mark claimed by another in the context of a commercial website will likely infringe upon the trade mark rights of the other.[19] Because domain names often function as marks, domain names that are the same or confusingly similar to another's mark can infringe that mark.[20] Domain names that infringe established trade marks and service marks are actionable in the United States under federal and state trade mark and unfair competition laws using traditional notions of trade mark infringement and trade mark dilution.

In 1999, Congress enacted the Anti-Cybersquatting Consumer Protection Act to provide additional remedies with which trade mark owners could combat cyber-squatting and cyber-piracy. The Anti-Cybersquatting Consumer Protection Act provides for *in rem* jurisdiction in order to provide a remedy in the case of absent or unidentifiable domain name registrants.

Where the domain name registrant is subject to the court's jurisdiction (see text, below), the Anti-Cybersquatting Consumer Protection Act provides enhanced monetary damages in the case of bad faith registration or trafficking in or use of a domain name that is identical or confusingly similar to a trade mark or is dilutive of a famous mark. Most states have enacted similar anti-cybersquatting statutes. Where bad faith is not present or cannot be demonstrated, the trade mark owner is left to rely upon traditional concepts of trade mark infringement and dilution and the traditional remedies provided therefore.

United States-based trade mark holders injured by domain name registrants also may initiate cyber-arbitration conducted pursuant to the Uniform Domain Name Dispute Resolution Policy (UDRP). The UDRP, promulgated by ICANN, is incorporated by contract into all domain name registration agreements. The UDRP requires the trade mark owner to demonstrate a legally recognized trade mark right and bad faith registration and use by the domain name registrant.

However, whereas the Anti-Cybersquatting Consumer Protection Act can provide monetary as well as injunctive remedies, UDRP cyber-arbitration can only offer the injunctive remedies of domain name cancellation and transfer. The value of a UDRP result also is limited in that it may be appealed directly to a court of law, or upset by a court proceeding instituted at some later time.

The overall look and feel of a website may be protectable as "trade dress",[21] being that aspect of U.S. trade mark law that protects the outward appearance and packaging of goods and services.

Trade mark rights also are implicated on the Internet through the use of web technologies such as hidden text, metatags, framing, linking and pop-up, banner, and search engine advertisements keyed off terms that function as marks. As discussed below, wheth-

---

[19] *Playboy Enterprises, Inc v Frena*, 839 F Supp. 1552 (MD Fla, 1993) (unauthorized dissemination of Playboy magazine photographs employing the terms Playboy and Playmate held to infringe Playboy's marks by confusing consumers as to whether Playboy authorized the dissemination, misappropriating Playboy's goodwill).

[20] *Brookfield Communications, Inc v West Coast Entertainment Corp*, 174 F.3d 1036 (9thCir, 1999).

[21] *Blue Nile, Inc. v. Ice.com, Inc.*, 478 F. Supp. 2d 1240 (D. Wash. 2007).

er or not use of these technologies infringe or constitute unfair competition depend upon the particular circumstances and the further development of law in this area.

As in the case of copyright law, First Amendment concepts of free speech and fair use may protect the limited use of another's trade mark though not authorized by the owner. So, for example, use of the phrase 'Playmate of the Year' by former Playmate of the Year Terri Welles was held protected as 'nominative fair use', although not authorized by Playboy, when used by Ms. Welles to describe herself in her website including in hidden meta tags that helped search engines locate her website.[22]

Patents

Like copyright protection, patent protection in the United States is solely a matter for federal law. Anyone who 'invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new or useful improvement thereof', is entitled to patent protection under United States law.[23]

To be eligible for patent protection, the invention must be novel[24] and unobvious when considered by those skilled in the relevant scientific discipline.[25] Unlike most other countries, where an application for patents must be filed prior to any public use, sale or publication of the invention, those seeking patents protection in the United States may file up until one year following the public use, sale or publication of the invention.[26]

A patent, once issued, empowers its owner to exclude all others from making, using, or selling the invention for the term of the patent.[27] In the case of utility patents, the United States patent term is currently 20 years from filing.[28]

Computer programs and software have long been considered patentable subject matter in the United States.[29] More recently, in *State Street Bank & Trust Co v Signature Financial Group, Inc*,[30] the Federal Circuit, being the exclusive court of appeals for patent matters, held that business methods are eligible for patent protection if they are novel, unobvious, and produce a 'useful, concrete, and tangible result'.

Still later, in *Ex Parte Lundgren*,[31] the Board of Patent Appeals clarified that business method patents need not be implemented through a 'technological art', that is, business methods may be patentable though not described and claimed in terms of a computer or computer network. As United States law presently stands, therefore, any business method that is new, unobvious and produces a useful, concrete and tangible result is eligible for patent protection without regard to the means through which the method is practiced.

---

[22] *Playboy Enterprises, Inc v Terri Welles*, 279 F.3d 796 (9th Cir, 2002).
[23] 35 United States Code, s 101.
[24] 35 United States Code, s 102.
[25] 35 United States Code, s 103.
[26] 35 United States Code, s 102.
[27] 35 United States Code, s 271.
[28] 35 United States Code, s 154.
[29] *Diamond v Diehr*, 450 US 175 (1981).
[30] *State Street Bank & Trust Co v Signature Financial Group, Inc*, 149 F.3d 1368 (Fed Cir, 1998), *cert. denied*, 525 US 1093 (1999).
[31] *Ex Parte Lundgren*, Brd Pat App, Number 2003—2088, October 2005.

No other country's laws or patent office has been willing to extend patent protection in respect of business methods to this degree.

Because software and business methods are patentable in the United States, issued United States patents can place significant restrictions on the manner in which e-commerce may be conducted. The Federal Circuit found Amazon.com's 'one-click' business method patent to be facially valid in *Amazon.com, Inc v Barnesandnoble.com, Inc.*[32] Similarly, Microsoft found itself sued for allegedly misappropriating Priceline.com's reverse auction business method protected by United States Patent 5,794,207, while the Blackberry personal information device had been embroiled until recently in litigation as a result of a claim by NTP, Inc that the email technology the Blackberry employs infringes upon NTP's patents.

Some scholars and politicians take the view that United States patent law goes too far and that the issuance and enforcement of business method patents harms the development of technology and e-commerce. Legislative efforts to reform the law are pending. Meanwhile, the U.S. Supreme Court decided a trilogy of patent cases in 2007 that, while not specific to business method patents, narrow the rights of patent holders generally.[33]

Trade Secrets

Trade secrets are protected, federally, through the Economic Espionage Act of 1996 and, in each state, through the Uniform Trade Secrets Act or analogous statute. A trade secret is generally any information the confidentiality of which has been safeguarded, that provides its owner with an economic advantage by being maintained in confidence and/or that would be expected to lose some or all of its value if publicly disseminated. A trade secret is misappropriated if used or disseminated in violation of an agreement, special relationship or confidence, or otherwise wrongfully acquired.

Actions for unlawful misappropriation of trade secrets have arisen in the context of the Internet, such as through the posting of another's alleged trade secrets on a publicly available Web site. Hacking into a secured website to unlawfully obtain confidential information having commercial value would constitute, among other things, misappropriation of trade secrets.

Federal and state laws prohibiting monopolistic practices, known in the United States as antitrust laws, limit the ability of businesses to extend the reach of their trade secrets through non-competition agreements. As with other forms of IP, constitutional safeguards also can limit an owner's ability to enforce its trade secret rights. In *Ford Motor Co v Lane*,[34] a federal district court declined to issue a preliminary injunction against the

---

[32] *Amazon.com, Inc v Barnesandnoble.com, Inc*, 239 F.3d 1343 (Fed Cir, 2001).
[33] *KSR Int'l Co. v. Teleflex Inc*., 127 S. Ct. 1727 (U.S. 2007)(clarifying and strengthening the non-obviousness standard which bolstered standard is now implemented in new USPTO examination guidelines); *MedImmune, Inc. v. Genentech, Inc.*, 127 S. Ct. 764 (U.S. 2007)(allowing licensees to challenge the validity of patents under license, without first being required to breach its license); and *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (U.S. 2006)(injunctive relief no longer always the appropriate remedy once patent infringement has been established).
[34] *Ford Motor Co v Lane*, 67 F Supp 2d 745 (ED Mich, 1999).

continued posting of Ford's alleged trade secrets based upon the First Amendment prohibition against prior restraint of speech.

Linking, Framing, Metatags and Trigger Ads

Generally, pointing to another's website without permission is in most instances not actionable. Pointing also, in most instances, will not cause secondary liability for infringing content posted on the pointed to website absent knowledge of the infringing content and motivation to promote infringement of that content on the part of the pointer.

Deep linking without authorization, ie, linking into an internal web page of a site in order to take commercial advantage, has been claimed to, and may in the appropriate instance constitute, unfair competition.[35]

Unfair competition also may result from framing another's site, depending upon the circumstances, motivation and results. Where framing, also referred to as in-line linking, is structured in a manner to cause or be likely to cause consumer confusion regarding source, origin or affiliation between the framed site and the framing site, the framing will likely be deemed actionable under trade mark or unfair competition law.[36]

In-line linking of copyright protected content has been held to constitute copyright infringement where, for example, a live audio webcast was made available for streaming through the linked website implicating, thereby, the copyright owner's performance right, [37] but not in the case of still photographs, because in-line linking only creates the impression that the content is hosted on the linked site's servers, when in reality it is not.[38]

Courts examining the practice of the sale by search engines of third party trade marks to competitors of the trade mark owner to trigger search engine results and banner advertisements, and also the practice by website owners of placing trade marks owned by competitor companies in metatags to trigger search engine results, have come out with inconsistent conclusions. Some have held that use of the trade marks in these manners does not constitute a use of the mark in commerce and, therefore, cannot support a case for trade mark infringement or dilution.[39] Others find these uses to be uses in commerce but which do not confuse the public.[40] These courts analogize the search results displayed using programs like Google's Adwords with the brick and mortar practice of placing competing brands side by side on department store shelves.[41] Still other courts find these uses to be uses in commerce which cause at a minimum initial interest confusion.[42] It is only this third category of courts that will allow actions for trade mark in-

---

[35] *Ticketmaster Corp v Microsoft Corp*, Number 97-3055 DDP (CD Cal, 28 April 1997).
[36] *Washington Post v Total News*, Number 97, Civ 1190 (SDNY, 5 June 1990).
[37] *Live Nation Motor Sports, Inc. v. Davis*, 2007 U.S. Dist. LEXIS 2196 (D. Tex. 2007).
[38] *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).
[39] *Rescuecom Corp. v. Google, Inc.*, 456 F. Supp. 2d 393 (D.N.Y. 2006)
[40] *J.G. Wentworth, S.S.C. Ltd. P'ship v. Settlement Funding LLC*, 2007 U.S. Dist. LEXIS 288 (D. Pa. 2007); *Boston Duck Tours, LP v. Super Duck Tours, LLC*, 2007 U.S. Dist. LEXIS 94681 (D. Mass. 2007)
[41] *Rescuecom Corp., note 41 supra.*
[42] *Tdata Inc. v. Aircraft Tech. Publrs.*, 411 F. Supp. 2d 901 (D. Ohio 2006); *Google Inc. v. Am. Blind & Wallpaper Factory, Inc.* 2007 U.S. Dist. LEXIS 32450 (D. Cal. 2007)

fringement and unfair competition based upon the practice of using another's trade mark to trigger search engine results and website ads to proceed.

Meanwhile, the state of Utah has passed legislation making it illegal to use another's trade mark to trigger online advertising. Given that this law would seem to impact interstate commerce, most expect the law will be stricken as unconstitutional.

Privacy Issues

In General

Protections against unreasonable governmental and private intrusions into one's personal privacy is afforded in the United States through provisions found in the constitutions of the federal and state governments, federal and state statutes, and state common law.

Some federal and state statutes are directed specifically to safeguarding privacy on computer networks. Others are directed to different subject matter, as for example financial and medical records, and impact the use of such subject matter over the Internet and in e-commerce.

Fair Information Principles and Industry Best Practices

In 2000, the Federal Trade Commission expressed[43] its expectation that consumer-oriented websites that collect personal identifying information from or about consumers online would comply with the five widely accepted fair information principles of:

- Notice (to the public of information practices);
- Choice (of how personal identifying information will be used);
- Access (to information collected about a person);
- Security (against inadvertent sharing or disclosure of the information); and
- Enforcement (against non-compliance).

While not themselves enforceable as such, the Federal Trade Commission fair information principles are often viewed as a benchmark for industry best practices for voluntary compliance and a standard by which common law tort standards of negligence and recklessness can be judged. Moreover, the Federal Trade Commission has and will take enforcement action for unfair or deceptive practices where a website claiming to be compliant fails in practice to comply with the fair information principles.

Common Law Invasions of Privacy

Most, if not all, states recognize common law torts of invasion of privacy, typically encompassing the following four varieties: unreasonable intrusion into seclusion, as for example via wiretap; the public dissemination of private facts; false light publications, being publications of fact in a manner to create false perceptions about a person; and the misappropriation of a person's name or likeness for a commercial purpose.[44]

---

[43] Federal Trade Commission Privacy Online: *Fair Information Practices in the Electronic Marketplace, A Report to Congress* (May, 2000).
[44] Restatement (Second) Torts, s 652A (1977).

Given the Internet's facility for public dissemination of personal information and likenesses, and the opportunities to conduct commerce using such information and images, it is not unusual to find publicly accessible content on the Internet that implicates one or more of these common law privacy torts.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act, a federal law, codifies law enforcement warrant requirements for the interception of electronic communications while at the same time creating privacy protections for stored electronic messages. Enacted in 1986, the law is intended to cover electronic mail operations, computer-to-computer data transmission, wireless devices, and private and public networks.

Title I of the Electronic Communications Privacy Act protects both voice and data communications streams, and includes storage of information incidental to transmission. Title I makes it a crime as well as a statutory tort to intercept a communication, disclose an intercepted communication, or use an intercepted communication, and prohibits public electronic communication services from intentionally divulging the contents of a communication to anyone other than the intended recipient. The Electronic Communications Privacy Act gives ISPs the liberty to intercept and disclose communications in order to conduct business, protect their networks, and cooperate with law enforcement.

Where one of the parties to a communication consents to its interception there is generally no violation of the Electronic Communications Privacy Act or other privacy law. Cases involving the placement of cookies brought under Title I of the Electronic Communications Privacy Act have focused upon whether the recipient of the cookie consented to it being placed on the recipient's computer.[45]

Title II of the Electronic Communications Privacy Act, also referred to as the Stored Communications Act, protects against the unauthorized access or disclosure of stored wire and electronic communications and transactional records. Included would be exceeding the authorization of an electronic bulletin board or a secured website, but only to the extent not accessible to the general public. Email messages stored by an ISP for purposes of backup have been protected by Title II of the Electronic Communications Privacy Act.[46]

The protections and penalties for stored electronic communications under Title II of the Electronic Communications Privacy Act are less severe as compared with the protections and penalties for electronic communications streams under Title I of the Electronic Communications Privacy Act. Title III of the Electronic Communications Privacy Act regulates the use of pen registers and trace devices when used for law enforcement purposes.

Computer Fraud and Abuse Act

---

[45] *In re Pharmatrack, Inc Privacy Litigation*, 329 F.3d 9(1st Cir, 2003).
[46] *Theofel v Farey-Jones*, 341 F.3d 978 (9th Cir, 2003).

The Computer Fraud and Abuse Act, also a federal statute, prohibits the unauthorized access of national security information and financial and consumer credit records residing on a computer, as well as the unauthorized access of a computer interconnected with the public network for purposes of taking things of value, if the value exceeds $5,000 in any one year period, causing harm or damage to persons, threatening the public health or safety, or altering, damaging or destroying information residing on a computer.

The Act, discussed in some detail in the section on fraud and computer crime, is frequently used to remedy the unauthorized access of a computer, computer network or secured portions of the world wide web, including by employers for acts committed by their employees.

Financial Information

The federal Gramm-Leach-Bliley Financial Modernization Act requires all financial institutions to ensure the security and confidentiality of customer records and information and protects against security threats and unauthorized access. The Act also precludes the sharing of personal information by financial institutions without the prior consent of the consumer.

Cable Subscriber Information

The federal Cable Communications Policy Act requires cable service providers to abide by prescribed fair information practices and to give subscribers notice of the company's privacy practices.

Health Information

The federal Health Insurance Portability and Accountability Act of 1996 regulates the use and disclosure of individual protected health information, including payment and insurance information.

The Health Insurance Portability and Accountability Act regulates anyone who handles or maintains such information, including when stored on and transmitted over the Internet.

Federal and State Privacy Acts

Federal and state privacy acts regulate the protection and disclosure of governmental records. These laws protect against the unauthorized disclosure of certain private information by government agencies and compel the disclosure upon appropriate request of non-confidential government maintained information.

Fair Credit Reporting Act and Financial Records Privacy Act

The federal Fair Credit Reporting Act limits the persons to whom consumer credit information can be disclosed and compels the disclosure of consumer credit information to concerned consumers upon appropriate request.

The federal Financial Records Privacy Act prohibits access to financial records by government authority except under enumerated circumstances.

Children's Online Privacy Protection Act

The federal Children's Online Privacy Protection Act of 1998, also discussed below, regulates the on-line collection of personal information from children under the age of 13, and it requires operators to obtain parental consent before collecting such information.

Unsolicited Bulk Email

In December 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM). CAN-SPAM makes it unlawful for a person to initiate a commercial email message that contains materially false header information, domain name or Internet protocol address, misidentifies the sender, or contains a misleading subject line.

The Act requires the sender to provide opt-out information and prohibits transmitting further unsolicited email after the recipient has objected. CAN-SPAM applies to commercial email only, and not to emails sent in the course of a continuing relationship or non-commercial emails sent for informational purposes. The Federal Trade Commission regards "commercial email" as only those emails that would constitute "commercial speech" within the meaning of the First Amendment.[47]

Actions for violation of CAN-SPAM may be brought by the Federal Trade Commission, other federal or state law enforcement agencies, or ISPs. While there have been some prosecutions under CAN-SPAM, CAN-SPAM has not substantially stemmed the flow of unsolicited bulk commercial email. One reason is that much of the SPAM reaching United States based recipients is initiated from places outside the reach of United States regulatory laws.

Many states have enacted their own anti-SPAM laws.[48] To the extent state anti-SPAM laws prohibit false and deceptive SPAM and include remedies beyond those provided by CAN-SPAM, the state laws are not preempted.

E-Annoyance law

Any person who communicates on the Internet without disclosing his or her identity with intent to annoy, abuse, threaten, or harass the recipient of the communication may be subject to criminal penalties under a 2005 amendment to the federal law that prohibits telephone harassment.[49]

Breach Notification and Encryption Laws

---

[47] 16 CFR s 316.3.
[48] Spam Laws: Summary, http://www.spamlaws.com/state/summary.shtml (last visited Feb. 10, 2008).
[49] 47 USC s 223(a)(1)(C) and 223(h)(1).

A majority of states have enacted laws requiring companies that store personal information on computer systems to notify customers after suffering a breach of security. States are also considering legislation that would provide civil, and sometimes even criminal, penalties for those who fail to encrypt computerized personal identifying information collected for business purposes.

Congress has been debating passing a federal breach notification law for several years now but has not yet managed to pass such a law. If passed, the law would have nationwide coverage and preempt inconsistent state law.

Employee Privacy Rights

United States courts examining the issue of employee rights of privacy in emails, voice mails and other information sent, received and stored on their employer's computers and equipment have generally found that employees have no expectation of privacy in such information.

The better practice is for the company to provide employees with clear written notice, through an employee handbook or otherwise, that information stored, sent and received from company computers and other equipment is not private and may be accessed by the company without notice to the employee.

Constitutional Protection

The federal and state constitutions protect against unreasonable government intrusion into personal privacy, generally arising from constitutional prohibitions on unreasonable searches and seizures.[50] This would include protection against unjustified intrusion by government into information stored on computers connected to the public digital network.[51] It also protects against the indiscriminate use of federal and state courts to compel information regarding the identity of individuals communicating over the Internet.

So, for example, those seeking to obtain the identity of authors of anonymous emails through subpoenas issued to the speaker's email service have been required to first demonstrate that (1) the speaker has been given notice of the subpoena, (2) the claim would survive a motion for summary judgment, and (3) a balancing of the parties' competing interests justifies disclosure.[52] Also, a federal court of appeals held that portions of the Stored Communications Act that purport to allow a court to order disclosure of the contents of stored emails without a warrant or prior notice to the subscriber are unconstitutional on their face.[53]

---

[50] *Katz v US*, 389 US 347 (1967).
[51] *State v. Reid,* 389 N.J. Super. 563 (App. Div. 2007)(a reasonable expectation of privacy exists in a Internet user's ISP account information); *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007)(holding that the Patriot Act's changes to the Foreign Intelligence Surveillance Act, permitting the government to wiretap without probable cause, are unconstitutional).
[52] *Doe v Cahill*, 884 A2d 451 (Del 2005); *Mobilisa, Inc. v. Doe*, 170 P3d 712 (Ariz Ct App 2007); *McMann v. Doe*, 460 F.Supp.2d 259, 263, 265 (D. Mass. 2006).
[53] W*arshak v. United States*, 2007 U.S. App. LEXIS 23741 (6th Cir. 2007).

However, third parties who cannot demonstrate a close relationship with an anonymous poster were held to be without standing to challenge such a subpoena on First Amendment grounds.[54] And notwithstanding the constitutional protections, record labels were permitted to subpoena universities for the identity of users of their Internet services alleged to have engaged in P2P file sharing of copyright protected content.[55]

Communications and Defamation

In General

Liability in the United States for false or misleading communications arises from common law causes of action for wrongful conduct known as 'torts'. Among these are the torts of defamation, intentional and negligent infliction of emotional distress, invasions of privacy, and general negligence.

These causes are all subjects of state, not federal, law, although cases stating such causes may be litigated in federal courts when, for example, the parties reside in different states and the amount in controversy is sufficient. While the details of the common law doctrines vary as between states, the underlying elements of each cause are substantially the same.

Defamation

Defamation can be defined as the non-privileged publication of a false statement to some third party which tends to injure the reputation of another. First Amendment free speech guarantees limit liability for defamation in certain cases, as for example where the victim is a public figure and the fallacy of the statement was the result of negligent and not intentional conduct.[56] Thus in *Carafano v Metrosplash.com, Inc*,[57] a federal district court dismissed a defamation action brought by a public figure actress against a matchmaker Web site for allowing the posting of false information about plaintiff where the Web site operator lacked the requisite information to have acted with malice in respect to the falsity of the information that had been posted.

Defamatory materials are easily published on or transmitted over the Internet. Prior to the enactment of the Communications Decency Act (see text, below), the operator of an electronic bulletin board who undertook to screen and censor postings was treated in the manner of a book publisher with editorial control and deemed to have liability for the defamatory content of the posting,[58] whereas an operator who allowed postings without oversight was treated in the manner of a book distributor and avoided such liability,[59] a result made certain by enactment of the Communications Decency Act.

---

[54] *Matrixx Initiatives, Inc. v. Doe*, 138 Cal. App. 4th 872 (Cal. Ct. App. 2006)
[55] *Arista Records, Inc. v. Does 1 - 4*, 85 U.S.P.Q.2D (BNA) 1154 (D. Mich. 2007); *Warner Bros., Records Inc. v. Does 1-4*, Copy. L. Rep. (CCH) P29,396 (D. Utah July 5, 2007).
[56] *New York Times Co v Sullivan*, 376 US 254 (1964).
[57] *Carafano v Metrosplash.com, Inc*, 207 F Supp 2d 1055(CD Cal, 2002).
[58] *Stratton Oakmont, Inc v Prodigy Services Co*, Number 21063/94 (Nassau County, 26 May 1955).
[59] *Cubby, Inc v Compuserve*, 776 F Supp 135 (SDNY, 1991).

Courts addressing defamation, right of publicity and right of privacy actions that concern content published on the Internet have applied the single publication rule applicable to print media, holding that the statue of limitations is measured from the first publication of the allegedly actionable content, notwithstanding reuses, multiple uses or continuing uses, where the content is used in each instance in the same or substantially the same manner.

Infliction of Emotional Distress

Intentional infliction of emotional distress typically requires an actor to engage in outrageous conduct with the specific intent to, or being substantially certain of, causing emotional distress in another, and the conduct succeeds in causing the target to suffer measurable emotional distress. Only some states recognize the tort of negligent infliction of emotional distress. When they do, they typically limit the tort to circumscribed situations, such as where the victim is in close spatial or relational proximity to a person physically injured by the actor's conduct.

Content published on or transmitted over public digital networks that is outrageous in character and that is intended by its publisher to shock and harm, and that does shock and emotionally harm, could cause the publisher or transmitter liability for intentional infliction of emotional distress.[60] Given the proximity requirements for a successful claim of negligent infliction of emotional distress, it is difficult to envision a situation whereby the publication or transmission of content over the Internet might give rise to a meritorious claim.

Privacy

The four varieties of common law torts for invasion of privacy are described briefly above in the Privacy section of this manuscript.

The Internet is an easy vehicle by which these torts can be committed and there have been a number of cases litigating invasions of privacy as a result of private or misleading materials, as well as likenesses, being published or posted on the Internet without the permission of the subject.

Negligence

The law of negligence imposes liability generally on anyone who fails to exercise reasonable care to prevent a foreseeable harm to a legally protected interest of another.[61] However, negligent conduct that results in pure economic injury, without attendant injury to persons or property, is in most cases unrecoverable. Thus, for example, tortious economic injury suffered by a subscriber due to lost business from down-time caused by negligence on the part of the subscriber's ISP is likely non-compensable, whereas lost

---

[60] *Stockdale v Baba*, 795 NE2d 727 (Ohio Ct App, 2003) (where a claim for intentional infliction of emotional distress was sustained against a man who had stalked two women and then continued to harass them by posting messages on a Web site message board naming the women and containing derogatory information about them).

[61] Restatement (Second) of Torts, s 281 (1964).

business where the ISP's negligence also damages the subscriber's computer may be recoverable. ISP subscriber agreements will, by contract, attempt to cut off the possibility of tort liability for any economic injury.

The law remains undecided whether negligence causing damage to data residing on a computer is damage to property and therefore compensable, or pure economic damage and unrecoverable in the absence of some injury to person or property. In *Lunney v Prodigy Services Company*,[62] the New York Court of Appeals rejected a negligence claim by a subscriber based upon Prodigy having failed to employ safeguards sufficient to prevent damage to the subscriber's reputation caused by an imposter opening subscriber accounts and posting offensive messages.

In the context of negligence actions brought by victims of security breaches against the companies that suffered the breach, the mere threat of possible future harm has been held to be sufficient to establish standing on the part of the victim but typically not be enough to sustain the action. Courts reviewing the issue have held, for example, that the cost of credit monitoring expenses does not meet the "economic loss rule," requiring instead some injury to person or property in order to make out a prima facie case. Where there has been some evidence of identity theft, together with a causal connection between the theft and the security breach, courts have been willing to sustain the action.

Other Actionable Wrongs

Liability for communications transmitted over the Internet can also arise from infringement of intellectual property rights, discussed above, product liability, which is strict liability arising from personal injury and property damages caused by defects in consumer products, the federal Fair Credit Reporting Act, discussed above, regulating the assembly, maintenance and dissemination of consumer credit information, false advertising, trespass-to-chattel, nuisance, and intentional interference with contractual relations or prospective economic advantage.

The tort of trespass to chattels has demonstrated limited, but versatile, utility in combating a variety of Internet wrongs. Trespass to chattels protects against unreasonable interference with the use and enjoyment of personal property. Where wrongful conduct does not deprive the person of the personal property entirely, but instead renders the property substantially useless to its owner, the tort of trespass to chattels has been committed. This tort has been used successfully to combat the use of 'spiders' or 'software robots' to mine data from another's website in *Register.com, Inc v Verio, Inc*,[63] and *eBay, Inc v Bidder Edge, Inc*,[64] finding that the spiders burdened claimants' computer systems, but not in *Ticketmaster Corp v Tickets.com, Inc*,[65] where the court found that there was no evidence of actual harm to Ticketmaster's computer system resulting from the robotic data collection.

[62] *Lunney v Prodigy Services Company*, 723 NE2d 539 (NY, 1999).
[63] *Register.com, Inc v Verio, Inc*, 356 F.3d 393 (2d Cir, 2004).
[64] *EBay, Inc v Bidder's Edge, Inc* 100 F Supp. 2d 1058 (ND Cal, 2000).
[65] *Ticketmaster Corp v Tickets .com, Inc*, 2000 US Dist LEXIS 12987 (CD Cal, 10 August 2000).

The unconsented to installation of spyware and adware on a computer was held to state a cause of action for trespass to chattels in *Sotelo v DirectRevenue, LLC*[66] and subsequent cases, while the mass emailing of critical comments to employees of Intel by a disgruntled former employee did not where the emails neither damaged Intel's computer system nor impaired its functioning.[67]

Communications Decency Act

The federal Communications Decency Act of 1996 substantially limits exposure to liability of Internet intermediaries for harmful content posted or transmitted by others. Section 509 of the Communications Decency Act instructs that 'no provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider'.[68] The Communications Decency Act further immunizes such providers and users from liability for restricting access to content that the provider or user considers objectionable, whether or not the material is constitutionally protected.[69]

The provisions of the Communications Decency Act have been construed by courts to protect ISPs, electronic bulletin boards, and other Internet intermediaries against a broad variety of torts, including general negligence and defamation torts,[70] invasion of privacy torts,[71] false advertising,[72] tortious interference with business relationships,[73] for an ISP's failure to remove objectionable material from an online discussion group,[74] for discriminating housing advertisements,[75] and for transmitting and, in some cases, manipulating, spam complaint reports,[76] although not for contributory or direct liability for trade mark infringement,[77] not where the intermediary participates in the provision of content,[78] not for creating a hostile work environment by allowing co-workers to view pornography on a company computer[79], not against unfair trade practice changes brought by the Federal

---

[66] *Sotelo v DirectRevenue, LLC*, 384 F Supp. 2d 1219 (ND Ill, 2005).
[67] *Intel Corp v Hamidi*, 30 Cal 4th 1342, at p 1347, 1 Cal Rptr 3d 32, 71 P.3d 296 (2003).
[68] 47 United States Code, s 230(c)(1).
[69] 47 United States Code, s 230(c)(2).
[70] *Zeran v America Online*, 129 F.3d 327 (4th Cir, 1997), *cert denied*, 524 US 937 (1998); *Ben Ezra Weinstein, & Co v America Online, Inc*, 206 F.3d 980 (10th Cir, 2000), *cert denied*, 531 US 824 (2000).
[71] *Doe v GTE Corp*, 437 F.3d 655 (7th Cir, 2003).
[72] *Perfect 10, Inc v CCbill*, LLC, 71 USPQ2d 1568 (CD Cal, 2004).
[73] *Corbis Corp v Amazon.com, Inc*, 351 F Supp. 2d 1090 (WD Wash, 2004).
[74] *Novak v Overture Servs*, 309 F Supp. 2d 446 (EDNY, 2004).
[75] *Chi. Lawyers' Comm. for Civ. Rights Under the Law, Inc. v. Craigslist, Inc.*, 461 F. Supp. 2d 681 (D. Ill. 2006)
[76] *Optinrealbig.com, LLC v Inronport Sys*, 323 F Supp. 2d 1037 (ND Cal, 2004).
[77] *GucciAmerica Inc v Hall & Associates*, 135 F Supp. 2d 409 (SDNY, 2001); *Ford Motor Co v GreatDomains.Com, Inc*, 60 USPQ2d 1446 (ED Mich, 2001).
[78] *Carafano v Metrosplash.com, Inc*, 207 F Supp 2d 1055 (CD Cal, 2002)(reversed upon a finding that the mere provision of a questionnaire into which content was input by a third party was insufficient to take hosting service outside the immunity provided by the Communications Decency Act, 339 F.3d 1119 (9th Cir, 2003)).
[79] *Avery v. Idleaire Techs. Corp.* 2007 U.S. Dist. LEXIS 38924 (D. Tenn. 2007)

trade Commission,[80] and not where the ISP aids and abets a crime through knowledge that otherwise lawful goods or services are being put to an illegal use.[81]

The CDA has also been held to protect individuals who post defamatory content authored by another, to protect those who publish knowing or having been warned of the offensive nature of the content, and also the operator of a social networking site which could have but failed to implement policies and technical features that might screen out objectionable content or protect minors from assault.[82] Without the CDA, websites like Facebook, MySpace and YouTube, whose functionality depends upon making user provided content available generally, would have infinite exposure and be short lived.

Claims for intellectual property infringement under federal law are specifically exempted from the immunity provided to web publishers by the CDA. There appears to be some disagreement as to whether this exemption applies equally to claims brought under state intellectual property laws. [83]

As discussed above, ISPs and other Internet intermediaries are immunized from liability for copyright infringement, by Title II of the Digital Millennium Copyright Act, when these operators and service providers duplicate, distribute, and transmit copyright protected materials in the normal course of providing Internet services.

Fraud and Internet Crime

In General

Fraud and Internet crime are regulated in the United States through both federal and state statutes. Some of these statutes are specific for crimes committed using the Internet while others are statutes that regulate criminal conduct generally and are implicated by activities performed using the Internet.

Criminal Copyright Infringement

Copyright infringement is punishable as a crime in the United States when done willfully and for financial gain.[84] The No Electronic Theft Act amended section 506 of the Copyright Act to provide that, where the infringement involves the reproduction or distribution, 'including by electronic means', of one or more copies having a total retail value of more than $1,000 during any 180-day period, so long as the infringing conduct was willful, criminal copyright infringement is committed even though not done for commercial gain.

The No Electronic Theft Act amendment was Congress' response to *US v LaMacchia*,[85] in which a federal District Court held that no crime had been committed where the de-

---

[80] *FTC v. Accusearch, Inc.*, 2007-2 Trade Cas. (CCH) P75,923 (D. Wyo. 2007)
[81] *Stoner v eBay, Inc*, 56 USPQ2d 1852 (Cal Super Ct, 2000).
[82] *Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843 (D. Tex. 2007)
[83] *Perfect 10, Inc. v. CCBILL LLC*, 488 F.3d 1102 (9th Cir. 2007)
[84] 17 United States Code, s 506.
[85] *US v LaMacchia*, 871 F Supp. 535 (DMass, 1994).

fendant had made available pirated software on the Internet for others to download without evidence that defendant was motivated by monetary profit or financial gain.

Wire Fraud

The federal wire fraud statute[86] makes criminal any scheme or artifice to defraud through the use of wire, radio or television communication in interstate or foreign commerce. The legislative history of the wire fraud statutes 'suggests that Congress wished to prohibit as much wire fraud as it could constitutionally make unlawful, limited only by the desire to avoid federal intrusion upon the police power of the states'.[87]

In order to establish wire fraud, the government must demonstrate, first, the formation of a scheme with the intent to defraud and, second, that the defendant somehow furthered the fraudulent scheme through the 'use of wire. . . communication'. Because the Internet is carried in substantial part by the public wire and radio communication networks, anyone who formulates a scheme to defraud some part of which is carried out over the Internet is guilty of criminal wire fraud. After the No Electronic Theft Act, this could include any willful scheme to infringe the copyright of another by means of the Internet.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act[88] makes it a crime to access one or more computers, any two of which are located in different states, without authorization or in excess of authorization, to cause certain enumerated results. Among these are obtaining government classified information or compromising a government owned or controlled computer; obtaining financial records; furthering a fraud unless the fraud involves only the use of the computer accessed; transmitting code intending to or in reckless disregard of a risk of damaging a computer if the conduct causes loss or damage of $5,000 or more in any one year period; modifying or impairing medical information; and trafficking in computer access passwords. Violations are punishable by up to 10 years imprisonment for a first offense, or up to 20 years for repeat offenses.

The Computer Fraud and Abuse Act has been used on at least one occasion to prosecute "wardriving", or piggy-backing on unsecured WiFi connections.

A private right of action with civil penalties also is available under the Computer Fraud and Abuse Act, and it is this aspect of the Computer Fraud and Abuse Act that has seen the most use. Hacking into a dating service website was held a violation of the Computer Fraud and Abuse Act in *YourNetDating, LLC v Mitchell*,[89] as was the sending of unauthorized bulk emails, impairing the performance of AOL's ISP facilities.[90]

The loss in the value of a trade secret resulting from a former employee's unauthorized access to and use of proprietary software was held compensable under the Computer Fraud and Abuse Act.[91]

---

[86] 18 United States Code, s 1343.
[87] HR Rep Number 388, 82d Cong, 1st Sess. 102 (1951).
[88] 18 United States Code, s 1030.
[89] *YourNetDating, LLC v Mitchell*, 88 F Supp. 2d 870 (ND Ill, 2000).
[90] *America Online, Inc v LCGM*, 46 F Supp. 2d 444 (ED 1998).

On the other hand, unauthorized access without evidence that information was acquired is insufficient to state a claim under the Computer Fraud and Abuse Act;[92] as is the mere act of placing cookies on computers without the knowledge or permission of the owner.[93] Courts are divided on whether an employee's unauthorized use of information that the employee was permitted to access can support a private right of action under the Computer Fraud and Abuse Act.[94] An employee accessing and using an employer's computer system in violation of an employment agreement or the employer's standards of conduct is actionable under the Computer Fraud and Abuse Act.[95]

A person with a single user license to a protected, subscription based website who shares his or her username and password with others for the purpose of allowing them to also access the website and its content may not only find him or herself liable for copyright infringement but may also be in breach of the Computer Fraud and Abuse Act.[96]

Electronic Communications Privacy Act

The Electronic Communications Privacy Act[97] renders it criminal to intentionally access without authorization a facility through which an electronic communications service is provided or intentionally exceed an authorization to access the facility and 'thereby obtain, alter, or prevent authorized access to the wire or electronic communication while it is in electronic storage of such system'.

Where the conduct is committed for the purposes of commercial advantage, malicious destruction or damage, or private commercial gain, violators are subject to imprisonment for up to one year for a first offense and two years for multiple offenses. Otherwise, the maximum prison term is six months.

Federal Wiretap Act

Intentional interception or disclosure of 'electronic communication streams' subjects the interceptor to imprisonment for up to five years.[98] Exceptions are extended to ISPs incident to their provision of services, for law enforcement, and other specified purposes.

Identity Theft

The Aggravated Identity Theft statute[99] prohibits knowingly using or possessing "a means of identification" of another person without lawful authority in relation to enume-

---

[91] *CH Robinson Worldwide, Inc v Command Transportation, LLC*, Case Number 05 C 3401, 2005 US Dist LEXIS 28063, (ND, Ill 16 November 2005).
[92] *PC Yonkers, Inc v Celebrations the Party & Seasonal Superstore*, 428 F3d 504 (3rd Cir, 2005)
[93] *Chance v Avenue A, Inc*, 165 F Supp 2d 1153 (WD Wash, 2001)
[94] *Brett Senior & Associates, P.C. v. Fitzgerald*, 26 I.E.R. Cas. (BNA) 674 (E.D.Pa. 2007).
[95] *Hewlett-Packard Co. v. Byd:Sign, Inc.*, 2007 WL 275476 (E.D. Tex. 2007).
[96] *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991 (E.D. Cal. 2007).
[97] 18 United States Code, s 3571(b)(3).
[98] 18 United States Code, s 2511(4).
[99] 18 USCS s 1028A.

rated felony offenses, and provides for a term of imprisonment of two to five years in addition to the term of imprisonment for the underlying felony offense.

Pornography Available to Children

In 1998, the U.S. Congress passed the Child Online Protection Act[100], which provides both civil and criminal penalties for transmitting sexually explicit materials and communications over the Internet that are available to, and harmful to, minors. In 2007, a federal trial court found the Act to be unconstitutional and permanently enjoined the federal government from enforcing the Act.[101]

Child Pornography

One who knowingly traffics in child pornography, defined as 'any visual depiction involving the use of a minor in sexually explicit conduct' over the Internet, is subject to imprisonment for up to 10 years.[102] The statute, which has been held constitutional based upon a construction that the defendant know the age of the performer,[103] is worded broadly enough to implicate those who merely establish a pointer on a web server to a notice or advertisement for child pornography located on another server.

The Child Protection and Obscenity Enforcement Act of 1998[104] seeks to regulate the use of underage models in the production of adult entertainment by requiring producers of adult material to maintain age records for each performer depicted as engaged in sexual activities and to label the adult material with information where such records are maintained. Regulations implementing this law have been interpreted to require websites through which the adult materials can be accessed to also provide the requisite information or to point to a website where the information is available.

While federal statutes only attempt to regulate child pornography, some states purport to regulate pornography more broadly as, for example, in Illinois through a statute prohibiting the publication of anything obscene[105] or in Michigan, through a statute criminalizing the knowing distribution of obscene matter to minors.[106]

Where the reach of a statute criminalizing the distribution of pornography is overbroad, it may be invalidated as encroaching upon First Amendment free speech rights.[107]

---

[100] 47 United States Code, s 231.
[101] *American Civil Liberties Union v. Gonzales*, 478 F.Supp.2d 775 (E.D. Pa. 2007). This ruling does not bind outside the court's district, and may or may not be followed by other federal district courts or federal appeals courts.
[102] 18 United States Code, s 225 1(c).
[103] *US v X-Citement Video, Inc*, 513 US 64 (1994).
[104] 18 United States Code, s 2257.
[105] Ill Rev Stat, ch 720, para 5/11-20.
[106] Mich Comp Laws, s 722.675.
[107] *Reno v American Civil Liberties Union*, 521 US 844 (1997) (striking down as unconstitutional that portion of the Communications Decency Act that sought to regulate the transmission of pornography over the Internet); *Ashcroft v Free Speech Coalition*, 535 US 234 (2002) (striking down as unconstitutional that portion of the Children's Online Privacy Protection Act that criminalized visual pornography).

Online Gambling

The federal government has been prosecuting those making available online gambling, whether from within or without the United States, under a variety of civil and criminal statutes including wire fraud, tax evasion and racketeering. In 2006, Congress passed the Unlawful Internet Gambling Enforcement Act, which seeks to stem online gambling by also making it unlawful to knowingly accept payments made by financial institutions on behalf of individuals engaged unlawful Internet gambling. Under this new law, credit card companies and those operating online payment systems can be prosecuted for facilitating bets over the Internet, Meanwhile, the United States' refusal to allow its citizens to engage in online gambling was sanctioned by the World Trade Organization as an unfair trade practice under the General Agreement on Trade in Services.

State Crimes

Comprehensive regulation of criminal conduct in the United States is provided by state, rather than federal law, and states generally retain concurrent jurisdiction with the federal government to prosecute cases where the criminal conduct transcends state borders.

Many states have statutes directed at computer and Internet focused fraud and other crimes that parallel the provisions of federal laws. State statutes also criminalize Internet related conduct not yet regulated by the federal government. New Jersey's recently enacted Internet Dating Safety Act, for example, makes it an offense to offer Internet dating services to New Jersey residents without informing them whether or not the service performs criminal background screenings and requires such services to educate their users about the dangers of Internet dating.

In addition, states are at liberty to prosecute behavior that violates a state statutory or common law criminal prohibition when carried out or otherwise facilitated through the Internet. The state law crimes of terroristic threatening, extortion, theft, and forgery all can be, and all have been, committed using public digital networks, as have others.

Creating Contracts Online

Contract creation and enforcement in the United States is primarily a matter for state statutory and common law. The common laws that govern contracts, described generally in the Restatement (Second) of Contracts (1981), are highly similar as between the states. Most states have, in addition, adopted certain uniform and model statutes in the area of contracting and commerce in order to further promote uniformity among their laws and advance commerce between states.

Probably the most important and most used of these uniform commercial laws is the Uniform Commercial Code. The Uniform Commercial Code governs most contracts for the sale of goods, as well as negotiable instruments, commercial paper, letters of credit, title documents, and secured transactions. Uniform Commercial Code, article II, governing the sale of goods, is intended to function between buyers and sellers located in different states in a manner not unlike the United Nations Convention on Contracts for the

International Sale of Goods is intended to function between buyers and sellers located in different countries.

The Statute of Frauds is a legal doctrine found in both state statutory and common law that requires contracts for more than a given amount of money, typically $500, as well as contracts of significant duration, generally one year or more, be memorialized in writing. Recently enacted federal and state electronic signature laws, discussed below, clarify that electronic documents and signatures satisfy the Statute of Frauds requirement for a writing.

A 1999 legal reform initiative intended that states would enact the Uniform Computer Information Transactions Act, a uniform law to govern contracts whose primary subject matter is computer information. A section of the Uniform Computer Information Transactions Act is dedicated to electronic contract formation. The Uniform Computer Information Transactions Act proved to be controversial and considerable debate ensued among scholars and state legislatures regarding the wisdom of its adoption. To date, only the states of Maryland and Virginia have adopted the law.

The Uniform Electronic Transaction Act (UETA), a uniform state law intended to govern electronic documents and signatures, fared substantially better than did the Uniform Computer Information Transactions Act and has been adopted by all but a few states. It incorporates those Uniform Computer Information Transactions Act provisions governing electronic contract formation. UETA endeavors to ensure that transactions in the electronic marketplace are as enforceable as transactions memorialized on paper with manual signatures, without changing the substantive rules that apply to contract formation and enforcement.

UETA borrows liberally from the United Nations International Trade Law Commission (UNCITRAL) Model Law on Electronic Commerce. It makes an electronic record legally equivalent to a paper record and a digital signature legally equivalent to a manual signature.

UETA does not compel parties to a contract to use electronic means. Both must agree that the transaction can and will take place electronically. UETA provides default rules for electronic transactions, and the parties are at liberty to opt out of some or all of the rules. Certain transactions and documents, such as testamentary documents, are ineligible for treatment under UETA.

UETA incorporates rules for when information is sent and received, what constitutes acceptance when an electronic agent (automated process) is used, and attribution of digital signatures. UETA authorizes parties to transactions to adopt any indication as a digital signature, including the ticking on click-through icons. UETA treats but does not require the use of digital signatures employing encryption and other security measures.

In June 2002, the federal government enacted the Electronic Signatures in Global and National Commerce Act (E-Sign) with the purpose of promoting electronic commerce among states pending the states' taking action. Like UETA, E-Sign validates the use of electronic documents and electronic signatures in place of paper documents and manual signatures in most cases and for most purposes.

E-Sign supersedes inconsistent federal and state laws, but does not require parties to contract electronically and includes protective provisions for consumers in the context of merchant/consumer transactions. E-Sign governs electronic transactions entered into by parties in states that have not yet adopted EUTA. Because E-Sign anticipated the adoption by states of EUTA, E-Sign expressively does not preempt or supersede EUTA. Rather, the laws mutually co-exist and may at times complement each other.

One area of electronic contracting that remains somewhat uncertain is the extent to which terms and conditions that employ click-through methods of acceptance are enforceable. Click-throughs or click-wraps have become commonplace methods of inviting acceptance of software licenses, ISP agreements, and when purchasing goods or services over the Internet.

While most courts considering click-through transactions have found them enforceable, United States courts will sometimes decline to enforce against consumers terms that are one-sided in favor of large merchants. Such contracts are characterized as 'contracts of adhesion' incorporating 'unconscionable' terms that favor the merchant while disadvantaging the consumer. In *Scarcella v America Online, Inc*,[108] a forum selection clause in an AOL membership agreement was held 'unreasonable' in light of the 'costs and inconvenience' of a consumer litigating a claim in a distant locale. In *Aral v Earthlink, Inc*,[109] the court found 'unconscionable' and unenforceable those provisions of a contract that forbade class action lawsuits and required a California based consumer to arbitrate across the country in Georgia. And in *Douglas v. United States Dist. Court,*[110] a federal court of appeals held that a provider of long distance telephone services could not change the terms of its service, in absence of notice to its customers, merely be posting the changes on its website.

Where a consumer is required by the structure of the merchant web page to scroll through the terms and conditions of the contract prior to indicating acceptance, courts are more likely to find the contract terms binding upon the consumer. To the extent courts have refused to enforce terms and conditions of click-through consumer transactions, those terms and conditions have generally been concerned with dispute resolution procedures, rather than matters affecting the substance of the contract. Terms that limit remedies and damages, also very commonplace in electronic transactions have, for the most part, been found enforceable.

Web crawlers and web bots have been held to enter into contracts with website owners simply by visiting the website and agreeing, albeit inadvertently, to the website terms and conditions.[111]

Jurisdiction and Dispute Resolution

In General

---

[108] *Scarcella v America Online, Inc*, Docket 5703 15/05 (NY Sup Ct, 28 December 2005).
[109] *Aral v Earthlink, Inc*, 134 Cal App 4th 544, 36 Cal Rptr 3d 229 (2005).
[110] *Douglas v. United States Dist. Court,* 495 F.3d 1062 (9th Cir. 2007).
[111] *Internet Archive v. Shell*, 505 F. Supp. 2d 755 (D. Colo. 2007).

Disputes arising from long distance commerce and communications facilitated over the Internet not uncommonly raise thorny issues of jurisdiction, venue, choice of law, and enforcement.

Federal Regulation of Internet Infrastructure

The Federal Communications Commission (FCC) has general authority over the nation's communications network pursuant to the federal Communications Act. Communications traffic is classified either as telecommunications services, subject to regulation, or information services, left for the most part unregulated. Thus far, the FCC has ruled that cable and wire-line broadband services are properly classified as "information services." As such, those who carry and provision Internet services are permitted to escape the burdensome regulation and oversight endured by most public utility companies in the United States.

The FCC meanwhile enunciated in the context of a non-binding policy statement "net neutrality" principles designed to promote and preserve an "open and interconnected public internet." The FCC has applied these principles when reviewing and approving mergers of telecommunication companies.

For purposes of the Communications Assistance for Law Enforcement Act (CALEA), however, the FFC classified broadband Internet carriage as "telecommunications providers." Consequently, Internet carriers are obliged to maintain historical information and to make that information available to law enforcement agencies according to the terms of CALEA.

The FCC has also asserted jurisdiction over the interconnected aspect of Voice Over Internet Protocol (VoIP) to require incumbent and local telephone carriers to interconnect and exchange traffic with VoIP carriers, and to require VoIP carriers to comply with some of the regulations that bind traditional telecommunications carriers as, for example, number portability and disability access requirements. A federal court of appeals has affirmed the FCC's position that states are without the right to regulate VoIP.[112]

Subject Matter Jurisdiction

Jurisdiction refers to the authority of the court over the subject matter and parties to a dispute. Subject matter jurisdiction is typically resolved by reference to the statute or common law to be enforced.

An issue that arises among the remote transactions facilitated by the Internet is to what extent the law of a given state can be applied to conduct occurring in whole or in part in another state. As concerns federal law, the issue becomes to what extent the federal laws of the United States can be extended to regulate conduct occurring in whole or in part in another country. Certain federal laws, in particular United States antitrust and intellectual property laws, have been applied to extra-territorial conduct.

Personal Jurisdiction

---

[112] *Minnesota PUC vs. FCC,* 483 F.3d 570 (8th Cir. 2007).

Issues of personal jurisdiction over parties to controversies arisen from e-commerce and Internet communications are typically harder to resolve than those of subject matter jurisdiction. Procedural due process guarantees found in the Fifth and Fourteenth Amendments to the United States Constitution limit the extent to which courts, federal and state, can assert jurisdiction over persons who are not citizens and residents of the locale in which the court sits.

There are two varieties of personal jurisdiction that comport with constitutional due process guarantees. The more broad variety is referred to as 'general jurisdiction'. General jurisdiction permits a court to take jurisdiction over a person who is 'generally present' within the state or district because the person is domiciled, has a place of business, is organized or consents to be sued there. The more limited type of personal jurisdiction is referred to as 'specific jurisdiction' and extends only to claims arising out of or related to a person's contacts with the forum state.

Consequent to constitutional due process guarantees, an out of state resident may only be compelled to answer process in a state if the non-resident's contacts with the forum state satisfy 'considerations of fair play and substantial justice'.[113] In concrete terms, this has been construed to mean that the claim that underlies the lawsuit is somehow related to the non-resident's contacts with the forum state and the circumstances are such that compelling the non-resident to answer legal process in that state would not be unfair.

Thus, for example, when a non-resident actively solicits business in another state, it is not unfair that courts in that state should take jurisdiction over the non-resident for claims that arise from the business resulting from the solicitation. Similarly, where tortious conduct is targeted at persons or property in a certain state, as when a tourist injures a resident while driving in another state, the courts of the state in which the victim resides and was injured may take jurisdiction over the out-of-state visitor.

These same general principles are applied to disputes that arise from e-commerce or other conduct or activities taking place on public digital networks. Courts considering disputes that arise from information posted on websites that are passive, the primary purpose of which is informational or promotional rather than to transact business, have generally found that the fact such content is accessible to and may injure persons in other states forms an insufficient basis to require the operator or publisher of the site to answer process in those other states.[114]

However, where the website is interactive, and capable of transacting business, disputes that arise from such transactions can form a basis for asserting personal jurisdiction over a non-resident defendant.[115] Assertions of personal jurisdiction over non-resident defen-

---

[113] *International Shoe Co v Washington*, 326 Us 310 (1945).

[114] *Bensusan Restaurant Corp v King*, 937 F Supp 295 (SDNY, 1996) (a district court in New York determined that it lacked personal jurisdiction over a Missouri based defendant premised upon a claim that the defendant's website, advertising a Missouri restaurant, infringed upon the claimant's trade mark rights in New York).

[115] *CompuServe, Inc v Patterson*, 89 F.3d 1257 (6th Cir, 1996) (Ohio court took jurisdiction over defendant residing in Texas for a dispute arising out of an electronic contract that contemplated performance in Ohio and that was consummated on a server located in Ohio).

dants are also appropriate where a remote defendant targets a claimant in the forum state through use of the Internet.[116]

The case of *Zippo Manufacturing Co v Zippo Dot Com, Inc*,[117] delineates a sliding-scale rule to be applied in making the determination of whether personal jurisdiction exists over a remote defendant in disputes arising from Internet communications or transactions.

> At one end of the spectrum are situations where a defendant clearly does business over the Internet, [giving the Patterson case as an example], and [a]t the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdiction[, citing *Bensusan]*.
>
> The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

The Zippo sliding-scale test is widely adopted and followed among courts, state and federal, when deciding whether to exercise personal jurisdiction over an out-of-state respondent in cases arising from e-commerce or other Internet activities.

The due process restrictions that limit the authority of courts to take jurisdiction over persons and businesses located in a distant state also limit the authority of courts to take jurisdiction over persons and businesses located in other countries. *Asahi Metal Industry Co v Superior Court of California*,[118] Accordingly, persons and businesses outside the United States should not have to answer process issued by a court located in the United States unless the person and business has had contacts with the forum in which the court is located, the claims relate to those contacts, and the circumstances are such that it would not be unfair to require the person or business to defend in the United States forum.

In Rem Jurisdiction

United States courts can in limited circumstances take jurisdiction over disputed property, or *res*, in lieu of taking personal jurisdiction over the persons who claim the property. Referred to as *in rem* jurisdiction, this particular type of jurisdiction is useful where those claiming the property are outside the jurisdiction of the court or cannot otherwise be located. Remedies available in *in rem* cases are limited to a determination of property ownership. In the absence of defendants, monetary damages are unavailable.

Provisions of the Anti-Cybersquatting Consumer Protection Act, discussed above, treat domain names as property when authorizing the taking of *in rem* jurisdiction by federal

---

116 *Panavision International v Toeppen*, 938 F. Supp 616 (CD Cal, 1996), *aff'd*, 141 F3d 1316 (9th Cir, 1990) (personal jurisdiction over non-resident defendant appropriate where non-resident defendant targeted a local business by registering a domain name similar to a mark belonging to the local business for the purpose of demanding money from the local business).
117 *ZipoManufacturingCo v ZippoDotCom,Inc*, 952F Supp 1119,at p 1124(WD Pa, 1997).
118 *Asahi Metal Industry Co v Superior Court of California*, 480 US 102 (1987).

district courts sifting in the district where the applicable domain name register is located, but only when personal jurisdiction cannot be established over the domain name registrant. Because the mere registration of a domain name is an insufficient contact to confer a court with personal jurisdiction over the registrant,[119] legal challenges to domain name registrations must typically be brought in the state or district in which the domain name registrant resides.

The *in rem* provisions of the Anti-Cybersquatting Consumer Protection Act provide an alternative particularly useful when the domain name registrant is located outside the United States, or where the registrant used a fictitious name, contact information or privacy service when registering the domain name. Domain name registrants wanting to avoid the reach of the *in rem* provisions can choose to maintain their domain names with registries or registrars located outside the United States.

Venue

Venue involves a determination of in which court(s), among several that possess both subject matter and personal jurisdiction, a dispute may be litigated. Venue rules focus on matters of convenience and venue is normally determined by reference to the statute being sued upon or the place of the act, omission, or event giving rise to the claim. In disputes arising from Internet communications and transactions, the place of the act, omission, or event giving rise to the claim will not always be clear.[120]

Parties may consent, in advance, to venue via forum selection clauses. Such clauses have, alternatively been found enforceable and unenforceable in online consumer transactions.[121]

Choice of Law

Disputes arising from e-commerce transactions between parties from different states raise the issue of which state's law governs. Conflicts of law are a matter of both state statutory and common law. Some statutes incorporate conflicts of law provisions. The Restatement (Second) of Conflicts of Law codifies the common law of conflicts generally applied by states.

In the case of tort claims, the laws of the state having the most significant relationship to the occurrence and parties are to be applied. This determination includes consideration of the place of the tortious act, tortious result, injury, and claimant's residence. In the context of contract claims, the law applied in the absence of a selection specified in the contract is the law of the state having the most significant relationship to the transaction and the parties. These conflicts of law rules, at times, give rise to clear results and, other times, the opportunity for the parties to argue issues of procedure.

---

[119] *Heathmount AE Corp v Technodome.com*, 106 F. Supp. 2d 860 (ED Va, 2000).
[120] *Reuber v US*, 750 F.2d 1039 (DC Cir, 1984).
[121] *Freedman v America Online, Inc*, 294 F Supp. 2d 238 (D Conn, 2003) (forum selection clause held enforceable against AOL subscriber due to no exceptional inconvenience); *America Online, Inc v Superior Court*, 108 Cal Rptr. 2d 699 (Ct App, 2001) (forum selection clause unenforceable against a California subscriber because the clause contravened California consumer protection laws).

Enforcement of Judgments

In cases where a court asserts jurisdiction over a non-resident respondent, assets available to satisfy any monetary judgment that may be rendered are typically available only in the respondent's place of domicile. Judgments rendered by federal and state courts in one state are enforceable in other states pursuant to the 'full faith and credit clause' found in the United States Constitution.

Exceptions to this rule arise when the court where enforcement is sought disagrees with the court rendering the judgment that the latter had jurisdiction over the non-resident respondent, or where the public policy of the state in which enforcement is sought precludes enforcing the judgment. These same two considerations are implicated wherever enforcement of judgments is sought as between countries, with public policy playing a somewhat more significant role.[122]

Alternative Dispute Resolution

There is strong support in American jurisprudence for resolving disputes through vehicles other than traditional civil litigation. The Federal Arbitration Act[123] endows agreements to arbitrate with a heavy presumption of validity and broad scope and bars those who have agreed to arbitrate from filing and prosecuting lawsuits. State arbitration statutes do the same.

As discussed above, however, where a term in a consumer contract requires disputes to be settled by arbitration, a court may nevertheless allow the consumer to pursue conventional litigation if the court deems the provision unconscionable or otherwise unfair.[124]

ICANN's UDRP procedure is an example of an alternative dispute resolution procedure that is agreed to between domain name registrars and registrants as a result of ICANN mandated provisions in domain name registration contracts.

Development of Internet Standards

The development of Internet standards in the United States has been left, for the most part, to independent bodies of experts and private industry groups. Voluntary bodies, such as the Internet Engineering Task Force and the Internet Society, discuss and formulate standards and protocols that are later adopted and integrated into industry practice. ICANN, a California private non-profit corporation, is empowered through a joint project agreement with the United States Department of Commerce to develop, operate and maintain the domain name server (DNS) system.

---

[122] *Yahoo!, Inc v La Ligue Conte le Racisme*, 169 F Supp.2d 1181 (ND Cal, 2001), recently reversed and remanded after its third visit to the Ninth Circuit, 433 F.3d 1199 (9th 2006), involving the offering over the Internet of Nazi paraphernalia in violation of French criminal law.

[123] 9 United States Code, ss 1 *et seq*.

[124] *Specht v Netscape Communications Corp,* 306 F.3d 17 (2d Cir, 2002) (where agreement to arbitrate in a click-through license was ambiguous).

Two arenas in which United States law palpably affects the development of Internet standards by private industry are law enforcement and antitrust.

The Communications Assistance for Law Enforcement Act, for example, requires providers of telecommunications services to adopt their systems to facilitate eavesdropping by law enforcement agencies. Federal law enforcement and intelligence agencies seek to limit the use of strong encryption by the private sector and to assure that suppliers of encryption technology make available keys or ‘trap doors’ to enable law enforcement to penetrate encrypted messages.

United States antitrust laws, primarily Sections 1 and 2 of the Sherman Act, protect against illegal combinations injurious to economic competition. The work of private standard setting groups not uncommonly implicates such laws. The Noerr Peimington Doctrine immunizes from antitrust liability private industry efforts to petition the government for favorable legislation.

However, where an interested party exercises decision making authority in formulating a product standard in the context of a private association comprising market participants, Noerr Pennington will not immunize the party from antitrust claims arising from the effect the standard has on the marketplace.[125]

In June 2004, Congress enacted the Development and Promulgation of Voluntary Consensus Standards Act to further shield standard setting organizations from antitrust liability. Organizations that comply with the law’s requirements of notice, opportunity to participate, balancing interests, access to information, consideration of views and substantial agreement, and the right to express and have a position considered, succeed in having their exposure for civil damages from antitrust law violations substantially reduced.

A participant’s ‘not inadvertent’ failure to disclose to a standards setting body that the participant has or has filed for patent protection on a proposed protocol or standard can result in a Federal Trade Commission enforcement action for violation of anti-trust laws. So, for example, where Dell lobbied a video electronics association for an industry standard incorporating Dell’s patented technology while failing to disclose that it held the patent, the Federal Trade Commission found that Dell’s actions violated section 5 of the Federal Trade Commission Act and issued a consent order prohibiting Dell from attempting to enforce the non-disclosed patent for a 10-year period.[126] And in *Broad Corp. v. Qualcomm Inc.*, a federal court of appeals reinstated claims for illegal monopolistic practices based upon a patent holder’s allegedly intentional false promise to license proprietary technology on fair, reasonable and non-discriminatory terms in the context of a consensus-oriented private standard-setting environment when the standards-setting organization relied upon that promise when including the proprietary technology in a standard.[127]

---

[125] *Allied Tube & Conduit Corp v Indian Head, Inc*, 486 US 492 (1988).
[126] *In re Dell*, slip op, Number 931-0097 (LEXIS, Trade Library, Federal Trade Commission file).
[127] *Broadcom Corp. v. Qualcomm Inc.*, 501 F.3d 297 (3d Cir. 2007).