CYBERSPACE LAW AND POLICY:

A PRIMER FOR STATE POLICYMAKERS

Prepared by the Cyberspace Law Committee of
the State Bar of California Business Law Section

TABLE OF CONTENTS

INTRODUCTION

The Cyberspace Law Committee of the California State Bar Association's Business Law Section is pleased to present this first edition of Cyberspace Law and Policy: A Primer for California Policymakers. The purpose of this primer is to provide an overview for members of the California Legislature and other policymakers of the legal issues arising in the rapidly developing world of the Internet, as well as a short summary of significant legislation that has been enacted or proposed to address those issues.

In some ways, the term "Cyberspace Law" is a misnomer. The Internet has become such a ubiquitous part of everyday life that it touches on every field of law: intellectual property, tax, commercial transactions, privacy, freedom of speech, criminal law, to name just a few. Cyberspace nevertheless continues to present new and unique challenges to our state, its business, and its citizens. The authors of this primer hope that it offers a useful introduction to these challenges and to the legal approaches that have been taken to deal with them.

The primer is composed of three main sections: a timeline of Cyberspace-related legislation and legal activity; a summary of major topic areas for legislation, and, finally, a glossary of relevant terms.

The legal landscape in Cyberspace is rapidly changing, and we expect regularly to update and amend this primer as new legal issues arise. The Cyberspace Law Committee welcomes any questions or suggestions for ways we can enhance this primer in the future.

Bennet Kelley
James Snell
Co-Chairs, Cyberspace Law Committee
California State Bar Business Law Section
April 2010

TIMELINE OF CALIFORNIA CYBERLAW

TIMELINE OF CALIFORNIA CYBERSPACE LEGISLATION

Denise Olrich
Robert Hawn

The California State legislature has been on the forefront of legislation relating to the Internet since its use became part of our daily lives. Following is a brief review of some highlights of the laws enacted in this area by California's state legislature in the past several years.

2003-2004 Legislative Session

Privacy Policies. AB 68 (Simitian D-Palo Alto) enacted the "Online Privacy Protection Act of 2003" (Business and Professions Code §§ 22575-22579) which required website owners to post a privacy policy explaining in detail how and when the website owner will share personal information of its user with third parties.

Spyware. SB 1436 (Murray D-LA) enacted new Chapter 32 of the Business and Professions Code, which outlawed the transmission of spyware and authorized civil actions by victims or by the California Attorney general.

Spam. SB 1457 (Murray D-LA) enacted Business and Professions Code § 1729.5, which prohibited deceptive commercial emails and provided for civil actions by victims or by the state Attorney General.

GPS. As use of global positioning system (GPS) technology started to gain public attention, AB 2840 (Corbett D-San Leandro) amended Civil Code § 1936 to establish the right to a "surveillance free" rental car. The bill required disclosure to a car renter of any tracking device in his or her rental vehicle, as well as express authorization before a rental company may disclose any information about the renter's use of the vehicle.

File Sharing. When file-sharing programs such as Napster became popular, SB 1506 (Murray D-LA) enacted Penal Code § 653aa, in an effort to stop illegal copying and sharing of files. This law criminalized the sharing of commercial recordings and audiovisual works without disclosure of the identity of the sender.

2005-2006 Legislative Session

WiFi. The newfound popularity of wireless Internet access was recognized with the passage of the WiFi User Protection Bill (Business and Professions Code Section § 22948.5; AB 2415 (Nunez D-San Diego), which required manufacturers of WiFi

equipment to include warnings to users regarding how they can use their security features to stop unauthorized access to wireless networks.

Pretexting. The practice of pretexting, which involves the sale or use of telephone records obtained by persons pretending to be actual phone company subscribers, was made criminal by SB 202 (Simitian D-Palo Alto). The bill enacted Penal Code § 638 and provided criminal penalties including up to one year in jail and fines from $2,500-$10,000.

2007-2008 Legislative Session

Data Breach Security Law. AB 1298 (Jones D-Sacramento) amended Civil Code §§ 56.06 and 1785.11.2 and repealed § 1798.29 to expand the protections of the data breach security law by covering medical and health insurance information. The bill required that notice of a security breach be given to consumers when medical or health insurance information is disclosed, without authorization, together with a patient's name. It also required a security freeze to be placed on an account within 5 days of a request by an affected person.

Cyberbullying. AB 86 (Lieu D-Torrance), which amended Education Code §§ 32261, 32265, 32270, and 48900, responded to the increased concern over bullying activities occurring on social networking sites. It expanded the definition of bullying contained in the Interagency School Safety Demonstration Act to extend to electronic acts and allowed school officials to expel a pupil for such behavior.

Electronic Harassment. AB 919 (Houston R-San Ramon) was prompted by the lack of sufficient clarity regarding the deliberate harassment of an individual by distributing his or her private personal information with the intent of having third parties contact or otherwise violate the individual's privacy. The bill's author illustrated the harassment the bill addresses by describing a person who received obscene phone calls after her picture, without her consent, was taken from her MySpace page and posted on Craigslist with a lewd advertisement. The bill added Penal Code § 653.2, which extended the crime of stalking and harassment to include its perpetration by use of an electronic communication device.

RFID. SB 31 (Simitian D-Palo Alto) added Civil Code §§ 1798.79-1798.795 in an attempt to prevent theft of magnetic information ("skimming") by expressly protecting personal information stored on identification cards in RFID format.

Internet Publication of Sex Offender Information. SB 1187 (Battin R-LaQuinta) amended Penal Code § 290.46 to create greater penalties for child pornography, in response to studies showing a correlation between child pornography and pedophilia.

It added certain offenses to those requiring the broadest disclosure on the Megan's Law website.

Piracy and Music Piracy. Two bills were enacted to address widespread problems of counterfeiting of DVDs and CDs and music piracy. AB 1394 (Krekorian D-Burbank) amended Penal Code § 350 to apply existing law concerning manufacture, sale or possession of counterfeit registered trademarks to any type of business entity (rather than to just a corporation); to expand the acts that constitute trademark violations to include offering for sale, transporting, or distributing counterfeit goods; to apply the definition of a "counterfeit mark" to unassembled components of any counterfeited article; and to establish a procedure for forfeiting counterfeited items. AB 2750 (Krekorian D-Burbank) amended Penal Code § 653w to increase restitution damages for music piracy to include the reasonable costs incurred by the owner, producer, or trade association to investigate the piracy.

Privacy of Medical Information. Two companion bills were enacted in response to reports of widespread breach of patient confidentiality. AB 211 (Jones D-Sacramento, Alquist D-San Jose, Kuehl D-Santa Monica, Torlakson D-Contra Costa) amended Civil Code § 56.36 and added Health and Safety Code §§ 130200-130205. The bill required health care providers to implement appropriate safeguards to protect patient medical information from unauthorized access, use, or disclosure. It established the Office of Health Information Integrity to impose fines for violations and the Internal Health Information Integrity Quality Improvement Account to receive penalty fund deposits, and it permitted civil actions by government attorneys. SB 541 (Alquist D-San Jose) added Health and Safety Code §§ 1280.1, 1280.2, and 1280.15 to increase penalties for medical confidentiality violations and required notice to the state if a violation is discovered.

Text Messaging. SB 28 (Simitian D-Palo Alto) amended Vehicle Code § 23810.3 and added § 23123.5 to make text messaging while driving illegal. Text messaging for these purposes includes email and instant messaging.

Mailed Consent for Telephone Solicitation. In an attempt to stem abuses associated with the use of misleading written permissions for telephone solicitation, particularly towards senior citizens, AB 2059 (Nunez D-San Diego) added a number of required disclosures to be included in such written permissions by amending Business and Professions Code § 17592 and adding Business and Professions Code § 17514.

2009-2010 Legislative Session

Electronic Discovery. AB 5 (Evans D-Santa Rosa) amended many sections of the Code of Civil Procedure and enacted the "Electronic Discovery Act," which established procedures to obtain discovery of electronically-stored information.

Computer Hacking. AB 22 (Torres D-Pomona) amended Penal Code § 502 to increase fines for felony convictions of knowing and unauthorized access to computers, systems, or networks.

High Technology Week. In deference to California's leadership in technology issues, ACR 52 designates the second week of May as annual California High Technology Week.

Internet Raffles. SB 200 (Correa -D-Santa Ana) permits authorized, nonprofit raffles to be advertised over the Internet.

Jurisdiction for Identity Theft Crimes. SB 226 (Alquist D-Santa Clara) amends Penal Code § 786 to effect prosecution of identity theft offenses when multiple identity theft offenses occur in multiple jurisdictions and provide that jurisdiction for all substantially similar such offenses, including any associated crimes connected to an underlying identity theft offense, is proper in any of the counties where one of the offenses occurred.

Other legislation was introduced relating to issues including privacy and data security, public officials' personal information, social networking, and intellectual property piracy, as California legislators continued to create new penalties for crimes occurring in cyberspace, and consider ways to protect California consumers and the privacy rights of individuals.

PRIVACY RIGHTS

PRIVACY POLICIES

Stephen L. Davis

Overview

A **privacy policy** is a policy adopted by a website owner that governs the website's collection, use, and disclosure of private information about the website's users.

Depending on the level of interactivity between a user and a website, a user may disclose a wealth of private, personal information about himself or herself to the website: names, phone numbers, addresses, email addresses, credit card information, social security numbers, and other personal or financial information. Personal information may be useful not only to the website owner, but to third parties that collect that information, aggregate it, and use it for their own marketing or commercial purposes. It may also be used for fraudulent or criminal purposes.

A privacy policy serves two purposes. First, it puts website users on notice of the website owner's information collection practices, and the ways in which users may limit or manage the collection of private information about them. A privacy policy also regulates a website owner's practices, and subjects a website owner to potential liability to the user and to government enforcement agencies for violation of its announced practices.

Privacy policies have become standard practice for websites of all kinds, but in the United States, at least, there is no single, uniform body of law or regulations that governs what they must say. Instead, a website owner, depending upon the nature and scope of its website's business, activity, or users, may be subject to a patchwork of federal, foreign, and state laws.

California is one of the leaders in this area, being one of the first states to enact a law setting forth mandatory guidelines for privacy policies.

Federal Law

To date, the United States has not adopted a single uniform law to regulate the content of online privacy policies. Instead, federal privacy protection is characterized by a medley of different federal laws and regulations, and varying enforcement mechanisms.

Federal Trade Commission Regulation. Despite the lack of comprehensive online privacy protection laws, the Federal Trade Commission has regulated website privacy practices since the beginning of online commercial activity in the 1990s. Even before the

passage of privacy policy regulations, the FTC commenced actions against website owners that published privacy policies but did not follow them.[1]

Children's Online Privacy Protection Act. In 1999, Congress enacted the Children's Online Privacy Protection Act (COPPA), which regulates the collection of personal information about children under the age of 13.[2] The FTC promulgated regulations to implement the statute.[3]

Under COPPA, every website that collects personal information from children under the age of 13 must follow certain practices:

- It must provide notice in a "clear and prominent place and manner" of what information the website collects, how it uses that information, and what its disclosure practices are;
- It must obtain verifiable parental consent prior to any collection, use, or disclosure of personal information about a child;
- It must provide, upon the request of a parent, a description of information collected or used, the opportunity to refuse to permit the use of the information, and a means for the parent to review any personal information collected.[4]

Violations of COPPA are treated as unfair or deceptive practices within the meaning of the Federal Trade Commission Act, and may be enforced by the FTC or by state attorneys general.[5]

Private Health Information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes privacy and security requirements on the collection and maintenance of personal medical record information. A website owner that collects or maintains medical record information may be required to incorporate HIPAA guidelines within its privacy policy. [6]

Personal Financial Information. A variety of U.S. laws prohibits or regulates the disclosure personal financial data. A website owner may be required, depending upon the nature of its business, to incorporate these laws within their privacy policies. Under

---

[1] *See In re GeoCities, Inc.*, File No. 9823015 (FTC Consent Order entered August 13, 1998).
[2] 15 U.S.C. §§ 6501-6506.
[3] 16 C.F.R. §§ 312.1-312.12.
[4] 16 C.F.R. § 312.4.
[5] 15 U.S.C. § 57a(a)(1)(B).
[6] 45 C.F.R. § 164.312 (2004).

the Gramm-Leach Bliley Act, for example, entities that qualify as "financial institutions" must post privacy statements regarding their collection of financial information.[7]

European Law

The European Union has taken a more aggressive role in role than the United States in protecting consumer privacy in website use. In 1995, the European Union adopted the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (commonly known as the EU Privacy Directive).[8]

The EU Data Protection Directive requires each EU Member State to adopt in its national laws the principles that are set forth in the 1995 EU Data Protection Directive. As a result, the national laws of each EU Member States include provisions that regulate the collection and use by commercial, business, and governmental websites of personal data about a person -- that is, information, such as name, address, credit card number, etc.[9] Among other things, these national laws require a website to obtain express consent to collect a web site user's personal data. They also require websites to take certain steps to protect the quality of data obtained from their users.

The European Union does not regard United States law as adequately protecting data privacy, so compliance with American laws may be insufficient if an American website owner collects data from citizens of EU member countries. The EU has adopted "safe harbor" guidelines, whereby U.S. businesses that voluntarily adhere to certain privacy principles may be entitled to a presumption that their policies provide an adequate level of privacy within the meaning of the EU Data Protection Directive.[10]

California Law

California enacted the California Online Privacy Protection Act of 2003[11], which requires commercial website operators that collect "personally identifiable information" about California residents to conspicuously post their privacy policy. "Personally identifiable information", as defined in this statute, includes information such as name, address, email address, telephone number, social security number, any other "identifier that permits the physical or online contacting of a specific individual", or any "information concerning a user that the website or online service collects . . . from the

---

[7] 15 U.S.C. § 6801 *et seq.*

[8] Directive No. 95/46/EC (Oct. 24, 1995).

[9] *Id.*, Art. 3(2).

[10] U.S. International Trade Administration Electronic Commerce Task Force, "Safe Harbor Principles" (Nov. 4, 1998), http://ita.doc/gov/ecom/menu.htm.

[11] Cal. Bus. & Prof. Code §§ 22575 *et seq.*

user and maintains in personally identifiable form in combination with an identifier described in this subdivision."[12]

The California law sets forth basic minimal requirements for such website operators:

- The website operator must identify the categories of personally identifiable information that the operator collects through the website or online service about users who use or visit the website.
- The website operator must describe the process by which a user may review and request changes to any personally identifiable information collected, if the operator provides such an option.
- The website operator must describe the process by which the operator will notify consumers who use or visit its site or service of material changes to the policy.
- The website operator must identify the policy's effective date.[13]

[12] Cal. Bus. & Prof. Code § 22577(a).
[13] *Id.* § 22575(b).

DATA SECURITY AND RETENTION

Robert V. Hale II

Overview

Traditionally, people have kept records in the form of paper, and locked valuable records in files and storage rooms. Today, information in cyberspace is stored in digital, or electronic form, on computers. The extraordinary ease with which such information can be accessed, copied, transmitted, or destroyed poses an enormous challenge to the security and retention of valuable data.

California has a long record of leading the nation in consumer protection legislation, resulting in a variety of laws addressing data security and retention. Unlike the federal Constitution, California's constitution expressly includes a right to privacy.[14]

Discussion

In August 2002, California became the first state to enact legislation requiring any agency, person or business that conducts business in California, and owns or licenses computerized "personal information," to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed). Originally introduced by Senator Peace as S.B. 1386, passage of Civil Code section 1798.82.20 subsequently led to similar legislation in thirty-nine other states and continued efforts to do so in Congress.[15]

Following the enactment of S.B. 1386, California became the first state to institute an Office of Privacy Protection.[16] This office provides guidance for businesses on how to protect themselves, their employees, and their customers from identity theft. Its website includes a California Business Privacy Handbook, along with recommended practices for security breaches and information sharing.

In July 2003, California enacted the Computer Security Act (CSA), which requires businesses and financial institutions to safeguard the personal information of individual consumers, and provides for a limited private right of action. Under the Act, any

---

[14] Cal. Const., Art. 1, § 1, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." (Amended Nov. 7, 1972, to add the word "privacy.").

[15] *See* Nat'l Conf. of State, State Security Breach Notification Laws as of January 25, 2008, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited August 21, 2008).

[16] *See* http://www.privacy.ca.gov/ (last visited March 8, 2010).

business that owns or licenses personal information about a California resident must implement and maintain reasonable security procedures and practices to safeguard such data against unauthorized access, destruction, use, modification, or disclosure.[17] In broadening the coverage of S.B. 1386, the CSA requires that businesses must disclose any breach of their computer security systems.[18] The private right of action under the CSA also invites the possibility of a plaintiff bringing a CSA claim as a predicate action under California's Unfair Competition Act (UCL or § 17200).[19]

Most recently, in October 2007, Governor Schwarzenegger signed into law AB 1298, adding medical information and health insurance information to the definition of personal information under S.B. 1386.[20] Concurrently, the Governor also vetoed AB 779, which would have placed additional burdens on any person, business, or agency that (a) sells goods or services to any resident of California; (b) accepts as payment a credit card, debit card, or other payment device; and (c) is not already subject to regulatory oversight under the Gramm-Leach-Bliley Act's rules about disclosure of nonpublic personal information.[21] The bill included detailed requirements related to the storage of payment-related data, including retention periods, disposal, and encryption.[22]

Conclusion

Given continued public and regulatory scrutiny over data security issues, and the California legislature's strong record in addressing such concerns, the Governor can likely expect alternate versions of AB 779 to reach his desk in the near future.[23]

---

[17] Cal. Civ. Code § 1798.81.5(b).

[18] Cal. Civ. Code § 1798.82(a).

[19] *See* Cal. Bus. & Prof. Code § 17200.

[20] Cal. Civ. Code § 1798.82(e)(4) and 1798.29(e)(4).

[21] *See* AB 779, Section 1724.4(c).

[22] *See* AB 779, Section 1724.4(b)(1)-(7).

[23] See Raymond G. Mullady, Jr. & Scott D. Hansen, *Identity Theft Litigation: A Roadmap for Defense and Protection*, 2008 UTAH L. REV. 563, 2008.

ONLINE PROFILING AND BEHAVIORAL TARGETING

Stephen L. Davis

Overview

Internet commerce enables businesses to gather information about their customers in ways that were never possible before. By interacting with, and even by merely visiting, websites, users may knowingly and unknowingly convey information about themselves to website owners. By tracking users' online activities and using this information, website owners can target their advertising to web users' specific interests. Online profiling and behavioral targeting consist of a number of different methods and practices by which website owners gather and use information about the visitors to their websites.

How Online Behavioral Profiling and Advertising Works

A visitor to a website typically leaves a trace of his or her visit in the form of a *cookie*. A *cookie* is a small text file that is created by one's visit to a website and saved on one's computer. The cookie contains information that identifies the website user's computer server and also may save information about the user's last visit to the website, such as the website pages visited, the time and duration of the visit, search queries made during the visit, and whether the website user viewed any advertisements on the website.

Software on the website owner's computer enables a cookie to be saved to the website visitor's computer. The next time the visitor visits the same website, the site recognizes the visitor's computer through the cookie, and the website can tailor the visitor's experience. Or, the cookie may contain information that is recognizable by a third-party network advertiser. The presence of the cookie may trigger the opening of specific advertisements either by the original visited website or by other websites.

Cookies, by themselves, do not contain or reveal personally identifiable information about a web visitor, but they may reveal private information about a person in conjunction with other information provided by the visitor about himself or herself to a website. For example, if a visitor, in addition to visiting a website (revealing information about his Web viewing activities in the form of a cookie) also voluntarily provides personal information, such as his name or credit card number, then his identity theoretically can be linked by the website (and possibly others) to his web viewing activities.

Federal Trade Commission Proposed Principles

In December 2007, the FTC published a report that proposed four self-regulatory principles for advertisers that engage in online behavioral targeting. After soliciting comments from a variety of industry sources, on February 9, 2009, the FTC re-issued its statement of principles in revised form. The principles announced by the FTC were:

- ***Transparency and control***: Behavioral advertisers should disclose their targeting practices and give consumers choice over whether to allow the practice.
- ***Reasonable Security and Limited Data Retention***: Companies should provide reasonable security measures so data does not fall into the wrong hands, and should retain data only as long as necessary.
- ***Consent to Material Changes***: Before using data differently from the company originally promised how to use it, the company should obtain the express consent of the consumer.
- ***Consent for Sensitive Data***: Companies should obtain affirmative express consent before using certain kinds of data for behavioral advertising, including data about children, health, or finances. [24]

Legislative Activity

Behavioral marketing has caught the attention of Congress, although to date Congress has not enacted laws specifically addressed to this activity. On July 9, 2008, the Senate Committee on Science, Commerce, and Transportation held a hearing on Privacy Implications of Online Advertising, at which it heard statements from a number of industry figures, including representatives from the FTC, Microsoft, the Center for Democracy and Technology, and Facebook.[25]

On December 7, 2009, the FTC began a series of three public "Exploring Privacy" Roundtables to address whether further regulation of behavioral targeting was needed. At the first meeting, FTC Commissioner Pamela Jones-Harbour characterized industry efforts at self-regulation insufficient and advocated comprehensive privacy legislation.[26] Some industry representatives, on the other hand, expressed the hope that new self-regulatory principles would obviate the need for regulatory action.

---

[24] The text of the report is at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[25] Statements of the participants can be accessed at http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=e46b0d9f-562e-41a6-b460-a714bf370171&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2008.

[26] Kate Kaye, *FTC Commissioner Harbour: "We have entered a digital arms race, and the current outlook is troubling"*, CLICKZ (December 7, 2009) *available at* http://blog.clickz.com/091207-163544.html.

The second roundtable was held on January 28, 2010, with further discussion on the challenges posed to privacy by consumer information collection practices. The third and final roundtable took place on March 17, 2010.

RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY

Nicole Ozer

Overview

Radio Frequency Identification (RFID) is a generic term for technologies that use radio waves to automatically identify people or objects from a distance of several inches to hundreds of feet. First used during World War II to differentiate between friend and foe aircraft, it emerged in the commercial sector in the 1970s to track products as they moved through the manufacturing sector and then to tag and track cattle and other livestock. However, in recent years, RFID technology has been increasingly considered for use in government-issued identification documents like passports, drivers' licenses, and student badges.

In 2005, awareness of RFID increased as major media outlets reported about the privacy and security concerns related to new RFID-embedded passports.[27] An attempt by a small school district in Sutter, California, to force students as young as five years old to carry RFID school badges[28] also sharply focused attention on the technology and its implications on privacy and personal security.[29] Amid this firestorm of attention on the privacy and security implications of RFID-embedded identification documents, several landmark RFID bills were introduced in the California legislature in the 2005 and 2007 sessions.[30]

In 2008, SB 31 (Simitian D-Palo Alto) was signed into law, criminalizing reading information stored in RFID-embedded identification documents without an individual's knowledge and consent.[31] SB 768 (Simitian D-Palo Alto), which would have ensured that all government-issued identification documents contain technological protections such as encryption to prevent personal information encoded on RFID tags

---

[27] *See, e.g.*, Bruce Schneier, ***Fatal Flaw Weakens RFID Passports***, WIRED, Nov. 3, 2005, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69453 (last visited March 8, 2010)..

[28] The Sutter story was covered extensively in the local, national, and international press. *See, e.g.*, Kim Zetter, *School RFID Plan Gets an F*, WIRED NEWS,, Feb. 10, 2005, *available at* http://www.wired.com/news/privacy/0,1848,66554,00.html (last visited March 8, 2010); Greg Lucas, *Students Kep Under Surveillance at School,* S.F. CHRON, Feb. 10, 2005, *at* B1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/02/10/BAGG0B8I4D1.DTL (last visited March 8, 2010)..

[29] *See* Mary Catherine O'Connor, *Surveys Reveal Dubious Consumers*, RFID JOURNAL, Feb. 17, 2005, *available at* http://www.rfidjournal.com/article/articleview/1409/1/1/ (noting that, based on a quantitative study of more than 7,000 consumers, "[t]he number of U.S. consumers who are aware of RFID technology is growing steadily, but so are negative perceptions of the technology—especially among women.").

[30] *See, e.g.*, SB 682.

[31] Cal. Civ. Code § 1798.79.

from being able to be read and copied from a distance, was vetoed by the Governor in October 2006 despite overwhelming bipartisan support.[32]

With the Department of Homeland Security currently urging border states like California to distribute "enhanced" driver's licenses[33] that contain long-range RFID tags that can be read from a distance of 30 feet and contain no technological protections to keep the information from being read, copied, and cloned without an individual's knowledge or consent,[34] issues related to RFID and other identification technologies will surely continue to appear before the California legislature in future sessions. The following document is a brief introduction to RFID technology and some privacy and security considerations.[35]

What is RFID Technology?

RFID technology, and its rebranded market segments of "smart cards," "smart chips," and "contactless integrated technology,"[36] are all based on the same core technology. RFID tags are comprised of tiny antenna-equipped computer chips that can be encoded with information such as someone's name or social security number or, in the case of commercial use, the type of product or its origin. These chips, some as small as a grain

---

[32] See Unofficial Ballot, http://www.leginfo.ca.gov/pub/05-06/bill/sen/sb_0751-0800/sb_768_vote_20060830_1140PM_sen_floor.html (unofficial Senate voting record); *Unofficial Ballot*, http://www.leginfo.ca.gov/pub/05-06/bill/sen/sb_0751-0800/sb_768_vote_20060821_1253PM_asm_floor.html (unofficial Assembly voting record). For the full text of the bill and further analysis, see ACLU of Northern California, *Landmark Privacy Bill Heads for Governor's Desk*, http://www.aclunc.org/news/press_releases/landmark_privacy_bill_heads_for_govenor's_desk.shtml.

[33] *See* Dep't of Homeland Security, *Fact Sheet: Enhanced Drive's Licenses (EDL)*, Dec. 5, 2007, http://www.dhs.gov/xnews/releases/pr_1196872524298.shtm.

[34] *See* K. Koscher et al.,*EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond,* 2008, http://www.rsa.com/rsalabs/node.asp?id=3557.

[35] For additional resources, see California Research Bureau, *Radio-Frequency Identification Document Advisory Panel Issues*, http://www.library.ca.gov/crb/rfidap/issues.html; Nicole A. Ozer, *Rights "Chipped" Away: RFID in Identification Documents,* 2008 STAN. TECH. L. REV. 1, *available at* http://www.aclunc.org/issues/technology/asset_upload_file647_7757.pdf.

[36] *See* Gene J. Koprowski, *Wireless Industry Defends RFID for Passports*, TECH NEWS WORLD, Apr. 25, 2005, http://www.technewsworld.com/story/42349.html ("The Department of State is not calling the passports RFID-enabled; rather, it calls them 'contactless smart-cards'… DHS avoids the term 'RF' [radio frequency] like the plague…."); Smart Card Alliance, *RFID Tags and Contactless Smart Card Technology: Comparing and Contrasting Applications and Capabilities*, http://www.hidglobal.com/documents/tagsVsSmartcards_wp_en.pdf ("Smart Card Alliance members developed this document to compare and contrast the applications and capabilities of the two technologies. The differences are important to keep in mind as the various forms of RF chip technology become pervasive in the market.")..

of rice, are then embedded in documents and objects.[37] The chip transmits its stored information to nearby RFID readers by sending it a radio signal. The chips do not alert anyone that it is transmitting this information or to what reader this information has been sent. There are several different categories of RFID tags, including "passive" tags, "active" tags, and "smart" tags.

"Passive" tags are so termed because they have no internal power source and perform no actions until they are awakened by the radio signal emitted by a reader. Studies from the United States Department of State have shown that tags envisioned to be read from a few inches can actually be awakened and read at distances of more than 20 feet, with other scientists demonstrating that they can be read at greater than 69 feet.[38] Since these tags have no internal battery, they are often small, easy to embed, quite cheap to produce, and long-lasting.

"Active" tags have their own battery source. They do not have to wait to be awakened by a reader but are capable of continually broadcasting their stored information to any reader(s) in range. They also have a much longer read range of several hundred feet--some of up to 750 feet depending on battery power. The batteries in these tags normally last several years.[39]

So-called "smart" tags possess the technological capability to include some forms of security protection for transmission of sensitive data. These chips are sophisticated enough to allow the layering of data protection processes, such as cryptography and authentication,[40] on top of the core radio frequency technology actions performed by the chip. However, these tags are only as "smart" as the decision makers who decide

---

[37] The Hitachi "Mu chip" is .4 mm square –small enough to be embedded in paper. Hitachi, Electronic Numbering of Products and Documents using the "μ-chip" (or mu-chip) supported by a Networked Database unleashes new Business and Life Style Applications that facilitate innovative Manufacturing, Distribution, Consumption, Tracking and Recycling operations, http://www.hitachi.co.jp/Prod/mu-chip/.

[38] Testing conducted by the U.S. State Department showed that smart cards with passive chips that had an intended read range of only 4 inches could actually be read from a distance six times as far — 24 inches — and could theoretically be read from more than 3 feet away. It has also been reported that readers can "eavesdrop" on legitimate reader-to-card communications from a distance of 30 feet. Gov't Accountability Office, *Radio Frequency Identification Technology in the Federal Government*, at 6, http://www.gao.gov/new.items/d05551.pdf. Scientists from Los Angeles-based Flexilis showed at DefCon in 2005 that passive RFID chips can be read at up to 69 feet. Brian Krebs, *Leaving Las Vegas: So Long DefCon and Blackhat*, WASHINGTON POST SECURITY FIX, Aug. 1, 2005, http://blog.washingtonpost.com/securityfix/2005/08/leaving_las_vegas_so_long_defc.html.

[39] Gov't Accountability Office, *Radio Frequency Identification Technology in the Federal Government,* http://www.gao.gov/new.items/d05551.pdf.

[40] Very generally, cryptography is the procedure to translate data written in plain text into ciphertext, coded text that requires access to a key or password to again be able to read the information in plaint text. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

what types of protections should be built onto these chips and how effective these protections actually are against privacy and security attacks.[41]

Recent Privacy and Security Attacks

There have been several well-documented examples of the privacy and security vulnerabilities of RFID- embedded identification documents and devices:[42]

2008: Researchers Cracked New United States Border Crossing and Enhanced Driver's License Identification Documents.

In the fall of 2008, researchers at the University of Washington and RSA Labs illustrated "systemic problems" with the new United States border crossing PASS Card and "enhanced" driver's licenses which had already been distributed in several border states and which the Department of Homeland Security was urging California to consider.[43] The research and report demonstrates how a lack of technological protections and proper shielding enables the RFID chips in these documents to be read, copied, and cloned at distances of 25-30 feet. As a result of their findings, the independent researchers strongly recommended that the Department of Homeland Security and other relevant entities "switch to another technology" that would have "stronger security and privacy properties."[44]

2007: Computer Security Firm Cracked HID Global ProxCards Used for Many Building Entry Card Systems

With a handheld device the size of a standard cell-phone, costing $20 in parts, a small computer security firm in Seattle showed just how easy it was to read and copy the information encoded on the building entry cards in HID Global ProxCards, the RFID-embedded access cards used at many public and private buildings across the nation.[45] With the push of a button, the personal information on the RFID cards could then be re-transmitted, "spoofing" the existence of an entry card and gaining access to the very

---

[41] See below for a discussion of some of the vulnerabilities of "smart" tags.

[42] For full analysis, see Nicole A. Ozer, *Rights "Chipped" Away: RFID in Identification Documents,* 2008 STAN. TECH. L. REV. 1, *available at* http://www.aclunc.org/issues/technology/asset_upload_file647_7757.pdf.

[43] See K. Koscher et al, EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond, 2008, http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/EPC_RFID/Gen2authentication--22Oct08a.pdf..

[44] *Id.* at 12.

[45] Paul Roberts, *RSA: Door cards – the enterprise's weakest link*, INFOWORLD, Feb. 13, 2007, http://www.infoworld.com/video/archives/2007/02/rsa_ioactive.html (video of Chris Paget demonstrating the RFID cloner at the RSA Security Conference)..

buildings or information that the RFID chips were intended to protect from unauthorized access. As researcher Chris Paget explained, "[a]s the system stands at the moment, I could walk past someone on the street, maybe stand next to them in an elevator, and I could grab their card id and get into the building."[46]

2006: Security Researcher Cracked the California State Capitol Identification Cards and Gained Access to Member-Only Secure Entrances

In August 2006, security researcher Jonathan Westhues brought the vulnerability of RFID-embedded ID documents literally to the steps of the Sacramento Capitol.[47] In the shadow of workers installing the final stages of a $2.5 million dollar investment in concrete barricades, posts, and other security measures to secure the perimeter of the California State Capitol,[48] Westhues read the RFID-embedded entry cards of two California state legislators. In a matter of seconds, the information from the RFID tag popped up on his laptop screen. He transmitted the information from his laptop, and with the high security door believing he was Assembly member Fran Pavley, he gained access to the California State Capitol.

2006: Security Researcher Cracked VeriChip, the RFID Chip Approved for Implantation in Humans

In February 2006, the VeriChip, an RFID-tag approved by the Federal Drug Administration (FDA) for implantation into humans, was cracked by Jonathan Westhues in less than two hours.[49] Westhues was able to read and clone the chip in the arm of a *Wired News* reporter in mere hours with a reader the size of an MP3 player and an antenna about five inches long. Since first cracking the VeriChip, Westhues has shown that even smaller technology, costing as little as $20 and requiring little skill to assemble, can be used to read and clone the chip.[50] Once the VeriChip is read and cloned, the copy could be used for whatever purpose was intended for the initial chip, whether it be identifying a patient or accessing a secured location.

---

[46] *Id.*

[47] *Cloning* RFID *Tags in Sacramento,* ABC 7 News, *at* http://www.youtube.com/watch?v=4jpRFgDPWVA.

[48] *See Capitol Building to be Ringed with Barricades*, SILICON VALLEY/SAN JOSE BUSINESS JOURNAL, Mar. 20, 2002, http://www.bizjournals.com/sanjose/stories/2002/03/18/daily35.html. This work was completed in 2006.

[49] Annalee Newitz, *The RFID Hacking Underground*, WIRED 14:05 http://www.wired.com/wired/archive/14.05/rfid_pr.html; Susan Kuchinskas, *The New Chiperati*, INTERNETNEWS.COM, http://www.internetnews.com/security/article.php/3582971.

[50] For information on Jonathan Westhues' work, *see* http://cq.cx/vchdiy.pl.

2006: Computer Expert Cracked RFID Chips Used in British E-Passport (2006)

In November 2006, the technology protections on three million British e-passports was cracked by software written in less than 48 hours and an RFID reader bought for about $500.[51] According to Adam Laurie, the computer expert that helped crack the e-passport,[52] the protections put in place to protect this sensitive information was the equivalent of "installing a solid steel front door to your house and then putting the key under the mat." The British government could have included an authentication feature in the new e-passport that likely would have prevented this attack, but chose not to do so.[53]

2005: Security Researchers Cracked RFID Chips in Exxon Mobil Gasoline-Payment Passes and Automobile Anti-Theft Devices

Using a home-brewed device costing a few hundred dollars, researchers at Johns Hopkins University cracked the security in the Exxon Mobil gas-purchasing passes and automobile anti-theft devices in 30 minutes.[54] Once they had the code, they used a laptop and a simple RFID device to charge their gas purchase to another person's account. The work at Johns Hopkins also revealed the security vulnerabilities of anti-theft car devices that use similar chips. This research was a surprise to many car owners, but probably not for many car thieves. Police believe that car thieves often successfully steal expensive cars, such as two of soccer star David Beckham's custom-designed BMW's equipped with anti-theft devices, by using software to spoof the RFID system.[55]

---

[51] Steve Boggan, *Cracked It!,* GUARDIAN (UK), Nov. 17, 2006, http://www.guardian.co.uk/idcards/story/0,,1950226,00.html..

[52] Adam Laurie is a computer expert and technical director of the Bunker Secure Hosting, a Kent-based computer security company.

[53] *See* Int'l Civil Aviation Org., *Technical Report: PKI for Machine Readable Travel Documents Offering ICC Read-Only Access*, Oct. 1, 2004, http://www.csca-si.gov.si/TR-PKI_mrtds_ICC_read-only_access_v1_1.pdf (describing technical measures for securing travel documents); Ari Juels et al., *Security and Privacy Issues in E-passports*, 2005, http://eprint.iacr.org/2005/095.pdf. For more information about the history of the e-passport, see ACLU, *How the U.S. Ignored International Concerns and Pushed for Radio Chips in Passports Without Security,* 2005, http://www.aclu.org/privacy/spying/15780res20050426.html.

[54] Peter Weiss, Outsmarting the Electronic Gatekeeper: Code Breakers Beat Security Scheme of Car Locks, Gas Pumps, SCIENCE NEWS, Feb. 5, 2005, http://www.sciencenews.org/view/generic/id/5866/title/Outsmarting_the_Electronic_Gatekeeper_Code_breakers_beat_security_scheme_of_car_locks%2C_gas_pumps.

[55] Robert Vamosi, *Gone in 60 Seconds-- the High Tech Version,* NEWS.COM, May 6, 2006, http://news.com.com/2100-7349_3-6069287.html.

Privacy and Security Implications of Insecure RFID Technology

The vulnerability of insecure RFID technology to surreptitious reading, copying, and cloning from a distance of many feet makes it an easy tool for inappropriate tracking, profiling, stalking, and identity theft. Concern about the impact of RFID technology on privacy, financial security, and personal and public safety is not limited to privacy advocates, but is shared by government organizations such as the Government Accountability Office (GAO), independent researchers who specialize in RFID technology, and even by segments of the technology industry itself.[56]

In May 2005, the GAO found that "the use of tags and databases raises important security considerations related to the confidentiality, integrity, and availability of the data in the tags, in the databases, and in how this information is being protected. Key privacy concerns include tracking an individual's movements and profiling an individual's habits, among others."[57] Similar concerns about both tracking and profiling were also detailed to the Department of Homeland Security in 2006 by its Data Privacy and Integrity Advisory Committee (Privacy Advisory Committee).[58] In its Final Report, released in December 2006, the Committee set forth a host of criteria for agencies to consider when deciding whether to use RFID technology in identification documents, including whether another type of technology could accomplish the goals with less privacy and security risks.[59] The Institute of Electrical and Electronics Engineers, a nonprofit group representing more than 220,000 United States electrical, electronics, computer, and software engineers, has also expressed serious concern, stating that "RFID systems present a unique technical and policy challenge because they allow data to be collected inconspicuously, remotely, and by unknown, unauthorized, or unintended entities."[60]

---

[56] Neville Pattinson, director of Technology & Government at Axalto Inc. of Austin, Texas, commented at the June 7, 2006 DHS Data Privacy and Integrity Advisory Committee that "it's inappropriate to use RFID technology for tracking and authenticating identities of people," He further noted, "You can think of RFID as an insecure barcode with an antenna." *See* Kim Cameron, *Homeland Security Privacy Office Slams RFID Technology*, KIM CAMERON'S IDENTITY WEBLOG, May 19, 2006, http://www.identityblog.com/?p=451.

[57] See id.

[58] The Privacy Advisory Committee was created to advise the Secretary of the Department of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues relevant to DHS that affect individual privacy, data integrity and data interoperability and other privacy related issues. See http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm for more information and activities of the Privacy Advisory Committee. Dep't of Homeland Security, *Privacy Office – DHS Data Privacy and Integrity Advisory Committee*, http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm.

[59] Dep't of Homeland Security, *Report No. 2006-02: The Use of RFID for Human Identity Verification,* at 12, http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.

[60] IEEE-USA, Developing National Policies on the Deployment of Radio Frequency Identification (RFID) Technology, Apr. 23, 2009, www.ieeeusa.org/policy/positions/RFID.pdf.

Industry representatives have also formally expressed worries that some forms of RFID technology significantly threaten privacy. The American Electronics Association (AeA) and leading technology companies have echoed the concerns that core RFID technology does not adequately protect privacy.[61] In a 2006 letter to the State Department and Department of Homeland Security regarding what type of machine readable technology should be deployed in the new border crossing card, the trade organization and companies explained that basic RFID that was designed for identifying pallets of goods and allowing rapid inventory tracking is "inappropriate for personal identification applications." Such RFID technology has a very long read range, on the "order of 30 feet or more," and would "perversely maximize the possibility…of an illicit actor 'tracking' a person at very long ranges."[62] The information on the tag could also be "surreptitiously skim[med]."[63] The letter urged the government agencies to reconsider whether to use basic RFID technology because its use "would potentially threaten individual U.S. citizen privacy."[64]

Conclusion

Organizations as diverse as AARP, ACLU, Eagle Forum and Gun Owners of California,[65] academic and independent researchers, and even the technology industry itself has expressed serious concern over the use of insecure RFID technology in government identification documents. The California legislature has always been on the forefront of balancing the potentials of new technology with safeguarding privacy, personal security, and public safety. As issues related to technology and government identification documents come before the legislature in future years, this document and its resources can help guide well-informed policymaking.

---

[61] RE: Privacy and Security Concerns with the use of EPCglobal UHF Generation 2 technology in the Western Hemisphere Travel Initiative Card Program, Jan. 30, 2006, http://www.aeanet.org/governmentaffairs/AeA_Letter_Jan_30_2006.asp (last visited July 8, 2009).

[62] Id.

[63] Id.

[64] *Id.* The DHS disregarded the concerns of the AeA and developed the new border crossing PASS Card with long-range insecure RFID technology which has now been shown to be highly susceptible to surreptitious reading, copying, and cloning.

[65] For list of RFID bill supporters, see http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_31_cfa_20080813_175323_sen_floor.html.

CONSUMER PROTECTION

SPAM AND SPYWARE

Bennet Kelley

Overview

Spam and spyware are two areas where California continued its customary role as the country's chief "laboratory of democracy,"[66] by being in the forefront on both issues – albeit with mixed results. In the case of spam, California's landmark 2003 ban on spam would have shut down all email marketing in the United States and led Congress to quickly pass the CAN-SPAM Act of 2003 to preempt it. California's anti-spyware legislation, however, quickly proved to be a model followed by other states.

Discussion

Initial California Spam Laws

One challenge in the spam debate is the fact that there is no uniform definition of spam. While in policy discussions spam is generally understood to refer to unsolicited commercial email (usually in bulk form), a study by the Pew Internet & American Life Project found that consumers consider spam to be any email they do not want (regardless of whether it is solicited).[67] The Congressional Research Service noted that the fact that spam is the Internet version of a Rorschach test, "add[s]to the complexity of devising . . . remedies for it."

California enacted the nation's first "spam" law in 1998, by passing Assemblywoman Bowen's AB 1676 (Chapter 865) which amended Section 17538.4 of the Business & Professions Code to require that intrastate unsolicited commercial email ("UCE") include an "ADV" or "ADV: ADLT" label in the subject line and also provide a toll-free number which the recipient could call to opt-out of future emails.

By 2003, it was estimated that spam was costing California businesses well over $1.2 billion dollars. At the same time, online advertising was a $7.3 billion industry with a substantial presence in California and the industry reached $23.4 billion in revenue by 2008 with email accounting for two percent of this total.[68]

---

[66] "California Adds To Reputation as Nation's Trailblazer," *USA Today* (September 25, 2002).

[67] Deborah Fallows, "Spam: How It is Hurting Email and Degrading Life on the Internet, Pew Internet & American Life Project (October 22, 2003) 10. Most spam statistics are based on consumer categorization and not any defined criteria.

[68] Based on Interactive Advertising Bureau data for 2003 and 2008.

In 2003, California enacted the nation's first "spam ban." Senator Murray's SB 186 (Chapter 487) created a new Business & Professions Code Section 17529 which prohibited the sending of UCE into or from California and established a private right of action with a civil penalty of $1,000 per violation. The bill defined UCE based on whether or not the recipient had consented to receive messages from the advertiser and not the sender. The ban likely would have shut down almost all email marketing in the United States as it was later acknowledged to be based on the false premise that email marketers merely sent advertisements to the advertisers' lists when instead marketers offered advertisers the ability to reach new consumers through their own lists.

Federal CAN-SPAM Act

Less than three months after SB 186 was signed, President Bush signed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act")[69]. In enacting the CAN-SPAM Act, Congress struck a careful balance between a marketer's First Amendment rights and the interest of consumers, which according to one of the sponsors of the Act, essentially "says that if you want to send unsolicited marketing email, you've got to play by a set of rules."[70] The CAN-SPAM Act is principally a disclosure statute requiring advertisers to include their address and an opt-out mechanism in all emails and prohibiting the use of deceptive subject lines, headers or routing information.

In 2005, the Federal Trade Commission ("FTC") reported to Congress on the "Effectiveness and Enforcement of the CAN-SPAM Act of 2003" which concluded that

> the Act has been effective in achieving two desired outcomes. First, the substantive provisions of the Act have mandated adoption of a number of commercial email "best practices" that many legitimate online marketers are now following. Second, the Act has provided law enforcement agencies and ISPs with an additional tool to use when bringing suit against spammers. The more than 50 cases brought to date by the FTC, the Department of Justice, state Attorneys General, and ISPs demonstrate CAN-SPAM's enforcement efficacy.

The CAN-SPAM Act preempts state laws "that expressly regulates the use of electronic mail to send commercial messages," but excludes from preemption state laws "to the extent [the state law] prohibits falsity or deception in any portion of a commercial electronic mail message" or are not specific to email.[71] The Fourth Circuit in *Omega World Travel, Inc. v. Mummagraphics, Inc.*, No. 05-2080 (4th Cir. Nov. 17, 2006), however, held that states may only regulate statements that are materially false since "allowing a

[69] 15 U.S.C. § 7701 et seq.
[70] 149 Cong. Rec. S. 5,208 (2003) (statement of Sen. Wyden).
[71] 15 U.S.C. §§ 7701(b) (1), 7704(5), 7707(b) (1).

state to attach liability to bare immaterial error in commercial emails would be inconsistent with the federal Act's preemption text and structure."

Following passage of the CAN-SPAM Act, California passed Senator Murray's SB 1457 (Chapter 571) in 2004, which amended Section 17529.5 of the spam law to allow recovery of statutory damages for email advertisements that (i) "contains or is accompanied by a third-party's domain name without the permission of the third party;" (ii) "contains or is accompanied by falsified, misrepresented, or forged header information;" or "has a subject line that a person knows would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message."

In addition to the Attorney General, both internet service providers ("ISPs") and recipients of emails in violation of this Section may bring a private action and recover their actual or "[l]iquidated damages of one thousand dollars ($1,000) for each unsolicited commercial email advertisement transmitted in violation of this section, up to one million dollars ($1,000,000) per incident," plus reasonable attorneys fees and costs. The court may reduce the civil penalty to a maximum of $100 per email or $100,000 per incident where the defendant has "established and implemented, with due care, practices and procedures reasonably designed to effectively prevent unsolicited commercial email advertisements that are in violation of this section." [72]

In 2005 the California spam law was further amended by Senator Murray's SB 97 (Chapter 247), amending Business & Professions Code Section 17529.5 again to make violations punishable as misdemeanor with a fine of $1,000 and up to 6 months in jail.

California federal district courts are split on the question of whether the amended law is preempted by the CAN-SPAM Act. In particular, the courts have disagreed over whether Section 17529.5 can avoid preemption without requiring plaintiffs to show each element of common law fraud, including reliance and damages.[73]

Spyware

Like Spam, "spyware" is a term that is not well defined. As the Congressional Research Service explains[74], generally spyware

---

[72] Section 17529.5 remedies language mirrors the language of Section 17529.2 spam prohibition, including limiting consumers' right of action to unsolicited email which may exceed the scope of the CAN-SPAM Act's preemption exception.

[73] *Compare Asis Internet Servs. v. Vistaprint USA, Inc.*, 617 F. Supp. 2d 989 (N.D. Cal. 2009) (section 17529.5 is not preempted, even though it does not require showing of reliance or damages) and *Asis Internet Servs. v. Consumerbargaingiveaways, LLC*, 622 F. Supp. 2d 935, 940-44 (N.D. Cal. 2009) (same) with *Hoang v. Reunion.Com, Inc.*, No. 08-3518, 2008 U.S. Dist. LEXIS 85187, *4-6 (N.D. Cal. Oct. 6, 2008) (finding that CAN-SPAM only allows state causes of action based on common law fraud and dismissing section 17529.5 complaint that does not allege reliance and damages).

> is used to refer to any software that is downloaded onto a person's computer without their knowledge. Spyware may collect information about a computer user's activities and transmit that information to someone else. It may change computer settings, or cause "pop-up" advertisements to appear (in that context, it is called "adware"). Spyware may redirect a Web browser to a site different from what the user intended to visit, or change the user's home page. A type of spyware called "keylogging" software records individual keystrokes, even if the author modifies or deletes what was written, or if the characters do not appear on the monitor. Thus, passwords, credit card numbers, and other personally identifiable information may be captured and relayed to unauthorized recipients.
>
> Some of these software programs have legitimate applications the computer user wants. They obtain the moniker "spyware" when they are installed surreptitiously, or perform additional functions of which the user is unaware. Users typically do not realize that spyware is on their computer. They may have unknowingly downloaded it from the Internet by clicking within a website, or it might have been included in an attachment to an electronic mail message (email) or embedded in other software.

Utah v. California Approaches

In 2004, Utah became the first state to enact "spyware" legislation, but in reality the law was primarily designed to protect local 1-800 CONTACTS from adware that generated competing offers while consumers were placing an order with them. The Utah law never went into effect as it was found to violate the Commerce Clause.[75]

The Utah law was viewed as an example of the perils of attempting to define evolving technology in legislation. California avoided this problem by defining conduct, not technology in enacting Senator Murray's The Consumer Protection Against Computer Spyware Act (SB 1436, Chapter 843). The Act prohibited the use of software on a third party's computer to

> (1) take control of the computer . . . (2) modify certain settings relating to the computer's access to or use of the Internet. . . (3) collect, through intentionally deceptive means, personally identifiable information . . . (4) prevent, without authorization, an authorized user's reasonable efforts to

---

[74] *Spyware: Background and Policy Issues for Congress*. Congressional Research Service (April 4, 2005).

[75] Stefanie Olsen, *Utah judge freezes anti-spyware law*, CNET News.com (June 22, 2004).

> block the installation of or disable software . . . (5) intentionally misrepresent that the software will be uninstalled or disabled by an authorized user's action, or (6) through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus software installed on the computer.

The Act also prohibited inducing a consumer to download an application through false representations that it is necessary for security or privacy or other deceptive means. The California law has served as a model for other state spyware laws.[76]

In 2005, Senator Murray introduced SB 92 which sought to amend the Act to (i) make a violation a misdemeanor; (ii) allow the Attorney General, a District Attorney, an ISP or consumer to bring a private right of action to recover actual damages or $1,000 in statutory damages for each violation up to a maximum $1 million penalty per incident; and (iii) provide immunity to anti-spyware software providers for identifying or removing applications from a user's computer. The bill failed in light of opposition to the private right of action and immunity provisions.

Federal Response

At the federal level, the FTC provided the initial impetus for spyware legislation through its 2004 workshop on spyware. The FTC forum did lead to Representative Bono's (R-CA) introduction of the "Securely Protect Yourself Against Cyber Trespass Act" (also known as the "Spy Act") to prohibit the use of spyware and require notice and consent for certain adware programs. The Spy Act passed the House overwhelmingly in both the 108th and 109th Congress only to stall in the Senate each time.[77]

The largest obstacle for the Spy Act, however, is that the need for legislation is undercut by the Federal Trade Commission's long held position that it has sufficient authority under the FTC Act to address spyware and the fact that both the FTC and state Attorney Generals have launched a number of enforcement actions against spyware companies (and faux anti-spyware companies).[78]

---

[76] Terri J. Seligman, "Legislative Round-up," iMedia Connection (December 8, 2005).

[77] The Spy Act was amended in the 99th Congress to eliminate the inclusions of "cookies" in the definition of spyware. H. Rep. No. 109-32 at 22.

[78] *See* Roy Mark, FTC to Congress: Lose the Anti-Spyware, Internet News, (November 5, 2004); Center for Democracy & Technology, *Spyware Enforcement* . At the November 2006 FTC forum on Consumers in the Next Techade, FTC Chairwoman Majoras reiterated the FTC's position that no new legislation was needed. Roy Mark, *FTC Mulling Next-Gen Tech Policy*, Internet News.com (November 6, 2006).

In 2008, however, spyware provisions were part of Title II of the "Identity Theft Enforcement and Restitution Act" ("ITERA").[79] ITERA addressed a number of cyber-crimes by authorizing criminal restitution orders for identity theft offenses; allowing prosecution of computer fraud offenses not involving interstate or foreign commerce; expanding the definition of "cyber-extortion" to include a demand for money in relation to damage to a protected computer, where such damage was caused to facilitate the extortion and imposing criminal penalties for malicious spyware and keystroke loggers.

[79] Public Law 110-326, 122 STAT. 3560.

PHISHING, PHARMING, AND OTHER DATA HUSBANDRY EXPLOITS

J. Anthony Vittal

Malware has become the bane of the Internet. No longer the realm of "script kiddies," 80% of all malware is now written for criminal purposes to obtain money through identity theft, hacking, or straightforward extortion. Illicit data gathering and related misconduct for criminal purposes has become big business – and everyone is a target.

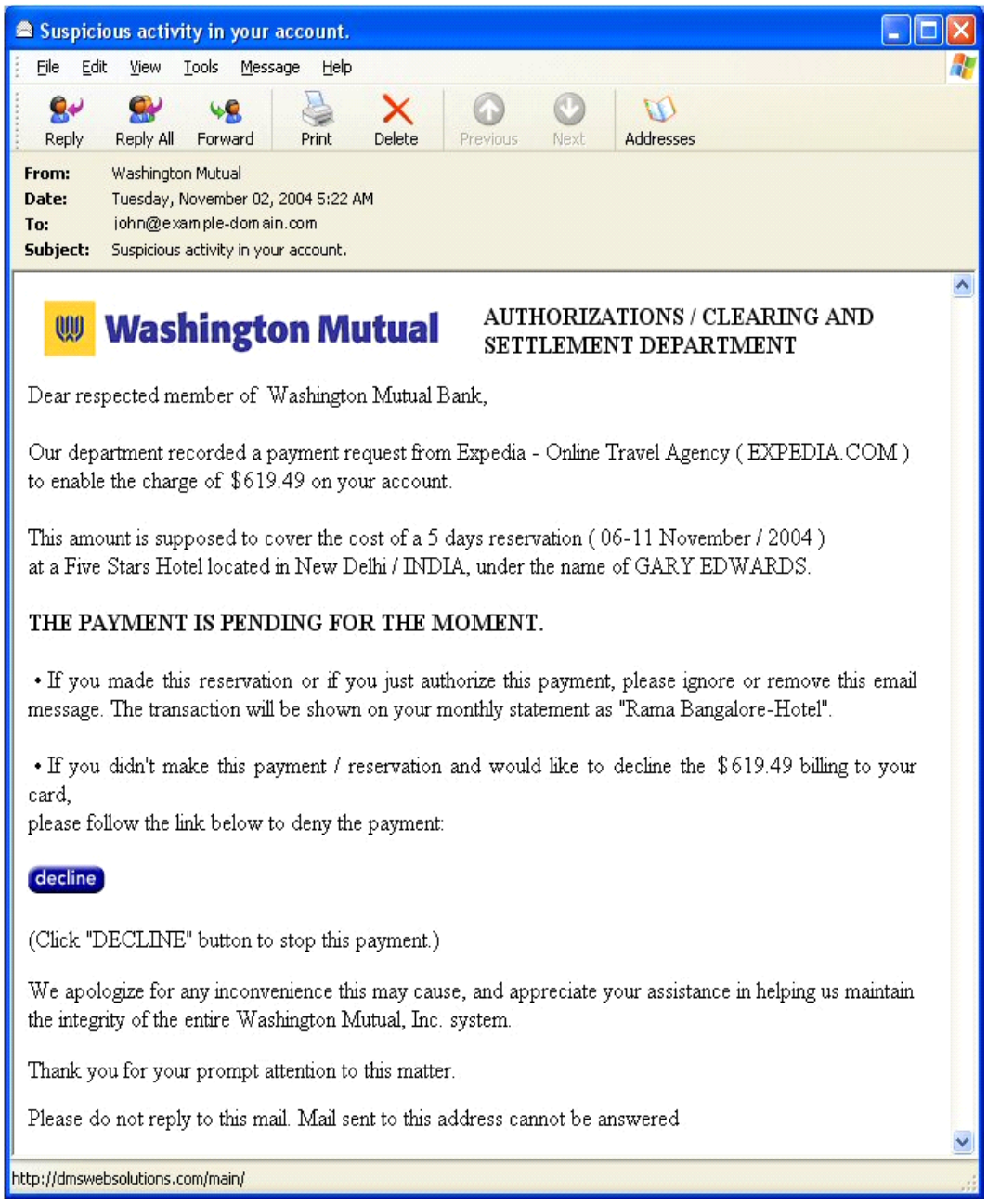
Overview

"Phishing" is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit card details, and other financial information by masquerading as a trustworthy entity in an electronic communication, employing both social engineering and technical subterfuge. "Spearphishing" is a highly-targeted variant of phishing, using the same techniques within a business enterprise or research facility to gain access to and ultimately steal confidential business information.

"Pharming" describes the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire administrative control of the domain name for a site, and to redirect that website's traffic to counterfeit websites operated by the phishers (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes). Pharming sometimes is described as the "corruption of navigational infrastructures."

Phishing

Who has not received an alarming email message, from a bank or brokerage house or on-line retailer with which you do business claiming that something is potentially wrong with your account necessitating immediate action? A more creative one reads:

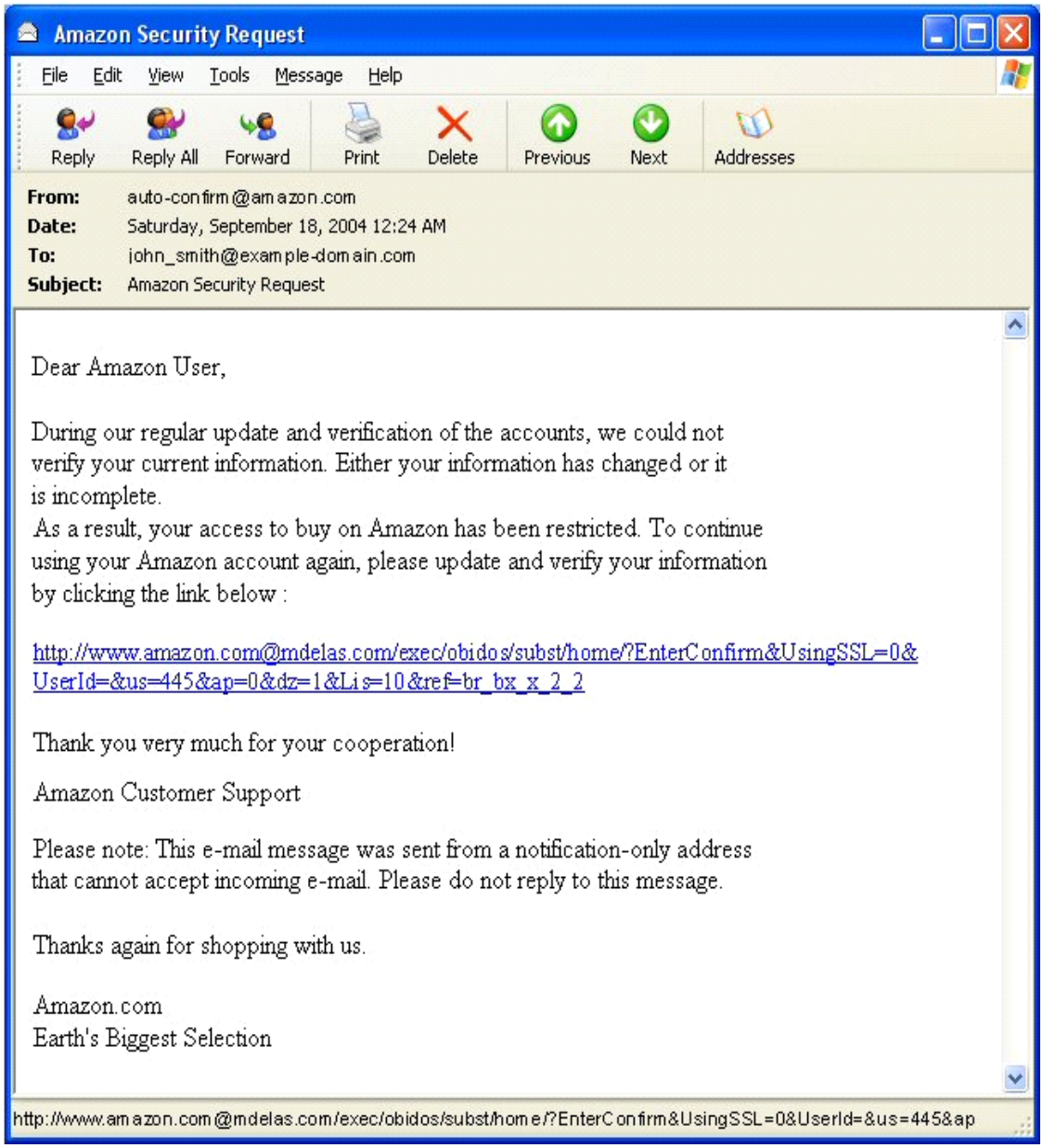


Even if you did not have a WaMu account, you would dismiss this out of hand. If you did, however, you might be tempted to respond – if for no reason other than to determine who Gary Edwards (the person for whom the reservation ostensibly was made) – unless you stopped for a moment to test the validity of the message.

As the following analysis reveals, this message is an actual phishing expedition. First, the language is arcane. When was the last time you were addressed in an email as a "respected member" of your financial institution? Second, you would expect an on-line payment transaction through Expedia to process automatically. Third, you likely would

expect an American institution to refer to a five-day (not 5 days) reservation at a Five-Star (not Five Stars) hotel. Finally, note the link at the bottom of the window – it does not point to the Washington Mutual website (*www.wamu.com*), but instead to *dmswebsolutions.com*, which clearly has no connection to WaMu. You certainly would expect an interstate financial institution to refer you back to itself, not a third-party domain, and would expect the institution to provide you a means of contacting it if you had any questions, rather than telling you not reply to the message.

Here is another:



The tip-off here is the URL in the link – *www.amazon.com@mdelas.com*. Since domain name servers look for the top-level domain at the end of the address or immediately to the left of the first "/" symbol, the link points to *mdelas.com*, not to *amazon.com*. *See* *https://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/privacy_security/fraud/page/fraud_examples* for other examples of phishing messages, using both SMS text messaging and email.

These messages all share a common goal – to prompt you to visit the linked website or to call the telephone number provided, where you will be asked for sufficient personal identifying information about yourself to enable the phishers to access and raid your account(s). The phishers all rely on the trust you have developed in the institutions with which you deal on-line. In some cases, the email may appear to come from a government agency, including one of the federal financial institution regulatory agencies or even the IRS. Many of the more sophisticated phishers even include links in their messages to legitimate portions of the actual institution's website – such as the privacy policy and the terms of use.

Phishing does not only have an adverse effect on consumers. Because phishing directly challenges the bond of trust between a seller's brand and its customers, it impedes the seller's marketing efforts and its ability to grow these on-line business channels.

The economics of phishing explain its popularity among identity thieves. Mailing and telephone number lists are readily available on the Internet for a relatively small investment. Phishers then run their messages through unsecured networks and proxy servers to hide the source information on their messages. It takes only a few "bites" at the bait to recover all of the costs incurred and to turn a profit. Even worse, some of the phishers are using their fake websites to deliver a Trojan horse backdoor program to your computer designed to give the phisher remote control of it, allowing access to all of your unencrypted data and enabling the phisher to use it to send more malicious messages.

According to the Anti-Phishing Working Group, the number of unique phishing reports received in August, 2009 was 40,621 – a three-fold increase from the 13,776 unique phishing reports received four years earlier in August, 2005. In August, 2009, APWG detected 56,362 unique phishing websites, up by an order of magnitude from four years earlier – despite the proliferation of anti-malware applications. Hijacked brands have increased five-fold over the same period to 341 brands in August, 2009.

The APWG report reveals other key data, reflecting changes in industry sectors targeted by phishers as aggressive defensive measures are adopted:

- The financial services industry remains the primary target of phishers, representing 54% of all attacks, down from 84.5% four years earlier.

- While ISPs represented the second largest target group in 2005, with phishers attempting to fool consumers into believing their Internet service would be terminated unless their credit card and other personal information is updated, ISPs now represent less than 3% of all targets.

- The payment services industry now represents the second largest target group at 26% of all attacks, followed by auction sites (8%), retail sites (3%), and others (9%).

- The U.S. continues to be the principal host to phishing websites, with an ever-increasing market share. By September, 2009, the USA hosted 75.76% of all phishing sites tracked by APWG. China and Hong Kong together hosted 9.93% of those sites. The rest of the top-10 list are Germany, the UK, the Republic of Korea, France, Canada, Russia, and Poland. Japan, Australia, and Sweden have fallen off the top-10 list.

- By August, 2009, the U.S. had lost its pre-eminent position as the principal host to websites hosting crimeware (malevolent software in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger). As of September, 2009, this category was led by China (26.9%), with the U.S. in second place (25.96%) and Russia in third place (17.88%). They are followed by Germany, Brazil, the Ukraine, the Republic of Korea, the Netherlands, Canada, and Spain.

"Nigerian" Advance-Fee Scams

According to the FTC, advance-fee fraud has been around for decades, but now seems to have reached epidemic proportions. Originally developed as the Spanish prisoner letters in the early part of the 20th Century, enterprising Nigerians elevated it to an art form. These email campaigns now are sourced in boiler room operations across Africa, Asia, and Europe. Some consumers have told the FTC they are receiving dozens of offers a day from supposed Africans politely promising big profits in exchange for help moving large sums of money out of their country. Apparently, many compassionate consumers are continuing to fall for the convincing sob stories, the unfailingly polite language, and the unequivocal promises of money.

These advance-fee solicitations are scams, and the scam artists are playing each and every consumer for a fool. The schemes work like this:

- Claiming to be government officials, businesspeople or the surviving spouses or children of former government honchos, con artists offer to transfer millions of dollars into your bank account in exchange for a small

fee. If you respond to the initial offer, you may receive "official looking" documents. Typically, the target then will be asked to provide blank letterhead and bank account numbers, as well as some money to cover transaction and transfer costs and attorneys' fees.

- The target may even be encouraged to travel to a country outside the U.S. to complete the transaction. Sometimes, the scammers will produce trunks of dyed or stamped money to verify their claims. Inevitably, though, emergencies come up, requiring more of the target's money and delaying the "transfer" of funds to the target's account. In the end, there are no profits to share, and the scam artist has vanished with the target's money.

Two rhetorical questions demonstrate the improbability of these schemes: Why would a perfect stranger pick you – also a perfect stranger – to share a fortune? Why would you share your personal or business information, including your bank account numbers, with someone you do not know? In addition, the State Department cautions against traveling to the destinations mentioned in the letters. According to State Department reports, people who have responded to these "advance-fee" solicitations have been beaten, subjected to threats and extortion, and in some cases murdered.

419 Scams

Working on the same social engineering principles as the "Nigerian" advance-fee fraud scams, so-called "419" pitches involve lotto schemes, prize claims, and other forms of fee solicitation initially delivered by email. Some of them are very creative, offering to donate a substantial portion of your "winnings" to charities of your choice to increase the probability of your response. Once again, "There isn't such thing as a free lunch."

Collection Actions

A creative new variant of these scams targets the legal profession. First, there is an email inquiry from a prospective client, located offshore, purporting to be an executive with a legitimate business enterprise, seeking legal counsel to collect a sizeable receivable from a customer. The ostensible client will sign an engagement agreement and sometimes even will provide a cost advance. The lawyer then sends a demand letter to the client's customer, threatening legal action if the debt is not paid, a resolution is negotiated, and the proceeds are deposited to the lawyer's client trust account. After the check "clears," the lawyer takes his or her contingent fee share and remits the balance to the ostensible client by wire transfer.

Several months later, the check turns out to be a forgery (since the "customer" and the "client" are co-conspirators), the bank on which the forged check was drawn demands repayment by the lawyer's bank, and the lawyer's bank empties out the lawyer's bank

accounts (including the trust account into which the forged check was deposited) pursuant to the bank's offset and recoupment rights against its depositor and, if the funds on deposit are insufficient to cover the loss, threatens the lawyer with litigation to collect the difference. In the meantime, the crooks are long gone with hundreds of thousands of dollars in ill-gotten gains in their pockets from a single transaction.

Pharming

The most insidious of the new data husbandry schemes is "pharming." In essence, a pharmer uses the vulnerability to fool the Domain Name System (DNS) into directing traffic destined for a legitimate website to the pharmer's illegitimate site – which looks just like the real thing. To understand this, you need to understand how the DNS works. A URL for a website (*e.g.*, *www.credit.com*) is the equivalent of a name in a telephone directory. To connect to a party, you need the telephone number and look it up in a directory. To connect to the computer associated with the URL *www.credit.com*, you need its IP address (*e.g.*, 64.127.114.195), which is provided by a DNS. Pharming substitutes a false IP address in place of the real one, and traffic gets re-directed.

Pharming attacks principally come in two varieties:

In a "DNS poisoning" attack, a hacker breaks into one or more DNS servers – *e.g.*, those operated by an Internet service provider – and replaces legitimate IP addresses stored in the server's cache with the IP addresses of bogus websites controlled by the hacker. Because these bogus websites typically appear to be clones of the legitimate websites, the user has no way of knowing anything is wrong. As a result, the operators of a phony banking site could easily capture usernames and passwords for every accountholder who is unknowingly redirected there.

An attacker can plant a virus, a Trojan horse, or some other malicious software (malware) on your computer. That program may capture and transmit your keystrokes, change your bookmarks and cookies, or change network settings to lead you to a fraudulent clone of the intended website. Once again, the crooks can extract a treasure trove of personal and account data from their unsuspecting visitors.

This danger is scarcely hypothetical. For example, according to the SANS Internet Storm Center:

- A pharming attack in early March, 2005, redirected visitors from at least 1,300 Internet domains to the compromised web servers. Log data from the compromised servers showed that the redirected requests came from more than 900 unique Internet addresses. In addition, more than 75,000 email messages were redirected.

- Another round of pharming attacks in late March, 2005 involved a DNS server, controlled by crooks, that presented itself as the authoritative DNS server for the entire .com top-level domain (*i.e.*, for all .com addresses). Since the DNS is designed to have all DNS servers talk to each other to keep the system up-to-date, other DNS servers were "poisoned" with the false IP address information, and they redirected all .com address requests to the crooks' pharm.

The "Troj/BankAsh-A" virus, delivered via attachments to spam emails, has diverted users of such online banking sites as Barclays, HSBC, Lloyds TSB, and NatWest to pharming sites. The attack is triggered by the virus itself, which lies in wait until victims try to visit their banking sites. Once the victim enters a username and password, the corresponding account is automatically emptied, and the funds are routed to the crooks' offshore accounts.

Another variant of pharming is index hijacking. In this scheme, pharmers spoof search engines (*e.g.*, Google and Yahoo) so that search results include links to phony websites that exist solely to download crimeware onto your system.

Rogueware

Rogue "antivirus software" is one of the most efficient – and increasingly preferred – ways to victimize consumers. As an example, one rogueware exploit starts with a link in or an attachment to a birthday greeting email sent to the victim. Clicking the link or the attachment icon launches the application (encoded with a unique binary), which not only bypasses detection by, but disables, the anti-malware software on the victim's computer and prevents it from updating; disables the system restore function on the victim's computer, hides itself in the victim's computer, and then displays itself to the user with an announcement that the victim's computer has been scanned, is infected by a virus, and offers a new (but bogus) anti-malware application for sale to "eliminate" the infection. A more insidious variant, known as ***ransomware***, literally locks up the victim's computer until a ransom payment is made for a "license" to free it from the cybercriminal's control. Some of these applications are designed to self-propagate, automatically infecting the rest of the computers on the victim's local area network.

The nastiest of these applications can irretrievably corrupt the registry on the victim's computer. As a result, absent paying the ransom, even if one can detect and remove the rogueware, the victim's computer is functionally unusable, requiring scrubbing and reformatting the drives, re-installing the operating system and all applications software, and then restoring the user's data files.

PRETEXTING

Jean Magistrale

Overview

Pretexting is a form of identity theft; it refers generally to a means of obtaining an individual's personal information under false pretenses. The practice of pretexting might also simply be called "lying;" that is, a pretexter lies about his or her identity or purpose in order to obtain privileged information from another person, usually by telephone, but sometimes also through email, customer service instant messaging, or a company website.

Discussion

A clever pretexter may use different tactics, depending on the type of information he or she is after and the sophistication of the "target" from whom he or she is seeking information. The pretexter may first establish trust with the targeted individual, then ask questions designed to gather key personal information. For example:

- A pretexter may obtain an individual's phone company records by calling the phone company and fraudulently pretending to be that individual.
- A pretexter may call an individual, claim to be from a research firm, and ask the individual for personal information such as name, address, social security number, or birth date.
- The pretexter might call a financial institution, pretend to be an account holder, claim to have forgotten his or her checkbook, and obtain information about the true account holder's account.

Using these various methods, a pretexter may be able to get credit in another person's name, steal another's assets, or investigate or sue another. Private investigators may use a form of pretexting to obtain information about the person being investigated, but not necessarily to steal their identity.

Some forms of pretexting are illegal under California and federal law, as discussed below. However, it is not illegal for a person to collect information about another individual that is a matter of public record, such as whether the individual owns a home, pays property taxes, or has ever filed for bankruptcy.

"Pretexting" is a new word that seemed to spring up suddenly, in connection with the Hewlett Packard scandal in 2006. It arose when the Chair of the Board at HP hired a firm of private investigators to obtain phone records of other members of the Board

after information about HP's long-term strategic plans appeared on the Internet. In response, the California Legislature enacted Penal Code § 638, discussed below.

California Law

California Penal Code § 638[80] outlaws the practice of pretexting to obtain phone records. It prohibits the purchase or sale of a "telephone calling pattern record or list" without the written consent of the subscriber, as well as the purchase or sale of records from VoIP calls, cell phones, satellite phones, and regular land line calls.[81]

Under the statute, a "telephone calling pattern record or list" is defined as information retained by a phone company that relates to the phone number dialed by the subscriber (or other person using the subscriber's phone with permission) or the number of an incoming call directed to the subscriber.[82] The definition also includes other data typically included on a subscriber's phone bill, such as the time a call started and ended, the duration of the call, any charges applied, and any information described in Public Utilities Code § 2891 (which includes personal calling patterns, numbers called by the caller, the subscriber's credit or personal financial information, services the subscriber purchases from the phone company, and demographic information about residential subscribers).

Obtaining phone records by fraud or deceit under the statute is a crime, punishable by fines up to $2,500 (or $10,000 for repeat offenders), imprisonment for up to one year in jail, or both.[83]

(Note that California's pretexting law is not intended to limit the scope or force of Public Utilities Code § 2891.[84] That statute prohibits a phone company from disclosing a subscriber's personal information to another person or corporation without the subscriber's consent.)

California's pretexting law is very similar to the subsequently passed federal Telephone Records and Privacy Protection Act of 2006, discussed below. Many of the federal provisions may preempt the California statute to the extent they cover the same conduct.

---

[80] An interesting historical note is that this same Penal Code section has been "recycled" over the years in accord with the then-current technology. When first enacted in 1872, it related to the neglect or postponement of delivery of telegraph or telephone messages. That provision was repealed in 1951, and then, in 1959, a new Penal Code § 638 was enacted which related to the operation of x-ray equipment in fitting shoes. That version of the statute was repealed in 1989. The most current version, relating to pretexting, was added by Stats 2006, ch 626 (SB 202).

[81] Pen C § 638(a), (b)(2).

[82] Pen C § 638(b)(2).

[83] Pen C § 638(a).

[84] Pen C § 638(h).

Federal Law

Phone Pretexting. The federal Telephone Records and Privacy Protection Act of 2006[85] contains similar provisions to California's Penal Code § 638, discussed above. The federal Act prohibits acquiring or attempting to acquire confidential telephone records of a telecommunications carrier or a VoIP provider by making false or fraudulent statements or representations.[86] It also prohibits the sale, transfer, purchase, and receipt of confidential phone records information.[87]

Criminal penalties under the federal law are more severe than the California statute, and include fines and prison sentences of up to 10 years, with double fines and an additional 5 years for repeat offenses within a 12-month period.[88]

Financial Data Pretexting. The Gramm Leach Bliley Act of 1999[89] prohibits fraudulent access to financial data. Under its provisions, a person may not obtain information from a financial institution relating to another person by making a fraudulent statement to an employee or a customer of the financial institution, or by providing a forged or fraudulent document to an employee of the institution.[90] It is also illegal to request another to obtain customer information of a financial institution, knowing that the person will attempt to do so illegally.[91]

RESOURCES ON PRETEXTING

California Penal Code § 638 (prohibiting phone pretexting)

Federal Telephone Records and Privacy Protection Act of 2006 (18 USC § 1039) (prohibiting phone pretexting)

Federal Gramm Leach Bliley Act of 1999 (15 USC §§ 6821-6827) (prohibiting fraudulent access to financial data)

Federal Trade Commission (FTC) website, "What Is Pretexting:"
http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/pretexting.hrml

Privacy Compliance and Litigation in California (Cal CEB 2008), chapter 4, "Internet and Electronic Privacy"

---

[85] 18 U.S.C. § 1039.
[86] 18 U.S.C. § 1039(a).
[87] 18 U.S.C. § 1039(b)-(c).
[88] 18 U.S.C. § 1039(b)-(e).
[89] 15 U.S.C. §§ 6821-6827.
[90] 15 U.S.C. § 6821(a).
[91] 15 U.S.C. § 6821(b).

Privacy Rights Clearinghouse on Gramm Leach Bliley provisions re pretexting: http://www.privacyrights.org/fs/fs24e-FinInfo.htm

"Whatis.com" definition of pretexting: http://searchcio.techtarget.com/sDefinition/0,,sid182_gci1215050,00.html

ONLINE RIGHTS AND LIABILITY

THE DIGITAL MILLENNIUM COPYRIGHT ACT AND USER-GENERATED CONTENT

Harry Boadwee

Overview

The federal Digital Millennium Copyright Act (DMCA)[92] amended the U.S. Copyright Act to provide significant immunities (or "safe harbors") from copyright infringement by online service providers. Among other things, these safe harbors have facilitated the tremendous growth online of "user-generated content" submitted by everyday people, including everything from photos and text to huge quantities of audio and video, now widely available over the web. However, they also have complicated the protection of intellectual property rights online, compared to the historic "offline" world where rights are cleared before publication.

Copyright Liability for User-Generated Content

Many websites and other online services rely heavily on content submitted by users (also known as user-generated content). Users submit not only home videos and amateur productions, but also content they have seen or heard elsewhere but do not own, such as content from media companies and other copyright holders. Under federal copyright law, the user placing the content on a website or online service without authorization from the content owner can be liable as a "direct" infringer.

The owners of these sites and services depend on Section 512[93] of the federal Digital Millennium Copyright Act (DMCA)[94] to protect them from legal liability for copyright infringement of such content.

Absent one of the four safe harbors of Section 512,[95] a service provider that hosts such content could be liable as a "contributory" or "vicarious" infringer (roughly analogous

[92] Pub. Law 105-304 (Oct. 20, 1998).
[93] 17 U.S.C. § 512.
[94] Pub. Law 105-304 (October 20, 1998).
[95] 17 U.S.C. §§ 512(a), (b), (c) and (d).

to being an accomplice of the user) or even a "direct" infringer.[96] Further, the service provider could face an injunction and large damages in a pre-set statutory amount.[97]

Summary of the Four Safe Harbors

*Threshold Requirement*s. To be eligible for any of the safe harbors, a service provider must meet the DMCA's threshold requirements. It must:

- Be a "service provider" as defined in Section 512(k).[98] The DMCA has two definitions for "service provider": a narrow one under the transitory communications safe harbor of Section 512(a), and a broader one for the other safe harbors.[99] Concerning the broader definition, one court observed that "'service provider' is defined so broadly that we have trouble imagining the existence of an online service that would not fall under the definitions."[100]

- Adopt and reasonably implement and inform its subscribers and account holders of a policy that provides for termination of repeat infringers.[101]

- Accommodate and not interfere with certain standard technical measures[102] developed in an "open, fair, voluntary, multi-industry standards process."[103] This process has not yet occurred.[104]

Transitory Communications Safe Harbor. This safe harbor[105] provides a broad limitation of liability, but covers only a narrow subset of ISP- or conduit-type service providers[106] who have merely a transient connection to the material.[107]

---

[96] According to one law professor, there is a "statutory ambiguity" as to whether the safe harbors "insulate all three flavors of copyright liability (direct, contributory or vicarious) or just direct infringement. … The interplay between the safe harbors and secondary infringement remains a multi-billion [dollar] statutory ambiguity." E. Goldman, "*Torrent Sites Induce Infringement and Lose DMCA Safe Harbor--Columbia v. Fung*," TECHNOLOGY & MARKETING LAW BLOG (Dec. 30, 2009), http://blog.ericgoldman.org/archives/2009/12/torrent_sites_i.htm.

[97] 17 U.S.C. § 504(c).

[98] 17 U.S.C. § 512(k).

[99] 17 U.S.C. §§ 512(k)(1)(A) and (B).

[100] *In re Aimster Copyright Litig*., 252 F.Supp.2d 634, 658 (N.D. Ill. 2002), *quoted in* B. Carver, *A Billion Dollar Test of the DMCA Safe Harbors,* CYBERLAW CASES, at fn. 8, available at http://cyberlawcases.com/2009/08/31/a-billion-dollar-test-of-the-dmca-safe-harbors.

[101] 17 U.S.C. § 512(i)(1)(A). For more examples and analysis of repeat infringer policies, see B. Carver, *supra,* at fn 4-7.

[102] 17 U.S.C. § 512(i)(1)(B).

[103] 17 U.S.C. § 512(i)(2)(A).

[104] See B. Carver, *supra*.

[105] 17 U.S.C. § 512(a).

[106] 17 U.S.C. § 512(k)(1)(A).

System Caching Safe Harbor. This safe harbor limits liability for technical methods of intermediate, temporary and automatic storage for purposes of indexing content and displaying such content (or excerpts) in online search results, among other things.[108] For example, Google's cache based on its index of web content has been protected under this safe harbor.[109]

Hosting Safe Harbor. This safe harbor[110] limits liability for copyright infringement "by reason of the storage at the direction of a user of material that resides on a [service provider's] network,"[111] as long as the service provider meets the following additional requirements:

- The service provider must designate an agent to receive notifications of claimed infringement and provide on its website and to the U.S. Copyright Office contact information for the agent.[112]

- Upon receipt of notification (containing specified details) from a copyright holder of claimed infringement, the service provider must respond "expeditiously" to remove (or "take down") the material.[113] This new "notice and takedown" procedure for user-generated content is a departure from the historic practice in the "offline" world of obtaining permission from the copyright holder *before* publication. (The original user who posted the material hosted on the service provider's website may file a counter-notification to oppose the removal.[114] The service provider is not liable for its good faith removal of material, subject to its compliance with other requirements of Section 512.[115])

- The service provider must not have "actual knowledge" of infringement;[116]

- The service provider must not be "aware of facts or circumstances from which infringing activity is apparent,"[117] the so-called "red flag"

---

[107] 17 U.S.C. § 512(a)(4).
[108] 17 U.S.C. § 512(b).
[109] *See Field v. Google*, 412 F.Supp.2d 1106 (D. Nev. 2006).
[110] 17 U.S.C. § 512(c).
[111] 17 U.S.C. § 512(c)(1).
[112] 17 U.S.C. § 512(c)(2).
[113] 17 U.S.C. § 512(c)(1)(C).
[114] 17 U.S.C. §§ 512(g)(2) and (3).
[115] 17 U.S.C. § 512(g)(1).
[116] 17 U.S.C. § 512(c)(1)(A)(i).
[117] 17 U.S.C. § (c)(1)(A)(ii).

knowledge.[118] In simple terms, the service provider should not take just a "wink-and-nod" approach to respecting others' copyrights.[119]

- Upon obtaining such knowledge or awareness, the service provider must "expeditiously" remove the material.[120]

- The service provider must not "receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity."[121]

Information Location Tools Safe Harbor. This safe harbor applies to copyright infringement by reason of the service provider "referring or linking users to an online location containing infringing material or infringing activity, by using [for example, an online] directory, index, … or hypertext link. …"[122] This safe harbor has additional requirements nearly identical to those of the Section 512(c) hosting safe harbor listed above.[123]

Relevance of Safe Harbors to User-Generated Content. The safe harbors of Section 512(a) and (b) are relatively technical and narrow. For purposes of copyright immunity for user-generated content, the hosting safe harbor of Section 512(c) is most relevant for the uploading and hosting of the content itself.[124] The information location tools safe harbor of Section 512(d) may be relevant to functions such as those enabling users to email or embed content elsewhere via a linking mechanism.[125]

Criticism and Litigation

Critics argue that the DMCA safe harbors make it too easy for copyright holders to force website operators to remove material from their sites, even if it is not infringing.[126] On the other hand, many copyright holders view the safe harbor procedures as a

---

[118] *See, e.g., Io Group, Inc. v Veoh Networks, Inc.*, 586 F.Supp.2d 1132, 1148 (N.D. Cal. 2008).

[119] *See* G. Sandoval, "*Reasons to care about Viacom v. Google*," CNET NEWS (March 19, 2010), http://news.cnet.com/8301-31001_3-20000815-261.html (discussing importance of red flag knowledge to the ultimate outcome of the *Viacom v. YouTube* case and the future of control of content online).

[120] 17 U.S.C. § (c)(1)(A)(iii).

[121] 17 U.S.C. § 512(c)(1)(B).

[122] 17 U.S.C. § 512(d).

[123] 17 U.S.C. §§ 512(d)(1), (2) and (3).

[124] *See* B. Carver, *supra*.

[125] *See* D. Given, *Clash of the Titans: Viacom v. YouTube*, DAILY JOURNAL (January 25, 2010).

[126] *See, e.g.*, F. Von Lohmann, *YouTube's January Fair Use Massacre,* ELECTRONIC FRONTIER FOUNDATION DEEP LINKS BLOG (Feb. 3, 2009), http://www.eff.org/deeplinks/2009/01/youtubes-january-fair-use-massacre. For practical approaches by copyright owners to address this issue, *see* F. Von Lohmann, *Viacom Gives Fair Use a Wide Berth on YouTube*, ELECTRONIC FRONTIER FOUNDATION DEEP LINKS BLOG (Apr. 23, 2007), http://www.eff.org/deeplinks/2007/04/viacom-gives-fair-use-wide-berth-youtube.

burden, since they must constantly scan online sites for infringing material and request its removal, which shifts the traditional burden of policing sites from the service provider to the copyright holder.[127]

Leading cases concerning the hosting safe harbor include:

IO Group Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132 (N.D. Cal. 2008), which held that a website that displayed videos submitted by users was protected under the hosting safe harbor, even though that site transcoded the videos into a new electronic format before displaying them.

Viacom Int'l Inc. et al. v. YouTube, Inc. et al, Case No. 07-CV-2103 (S.D.N.Y. 2007). Viacom, a media company that owns Paramount Pictures, DreamWorks and many cable channels, contends that YouTube infringed its copyrights by, among other things, failing to provide mechanisms to prevent users from posting infringing videos on a "massive" scale to the leading video sharing site on the web. In its complaint, Viacom alleged that it had identified more than 150,000 unauthorized clips of its copyrighted programming on YouTube that had been viewed 1.5 billion times, and requested damages of at least one billion dollars.

Advancing technology may have undercut much of the rationale for this litigation. YouTube has implemented an improved filtering system, called ContentID, which enables it to analyze content uploaded by users and compare it against a database of similar (but not necessarily identical) content owned by copyright holders.[128] If there is a close match, YouTube notifies the copyright holder, who can elect to share the related advertising revenue earned by YouTube. In other words, "rights holders can earn a cut off of videos they didn't even upload."[129] News reports indicate that a third of the advertisements on YouTube now are served beside copyrighted content found through this system,[130] with revenue shared with over a thousand media companies.[131]

---

[127] "[YouTube] has decided to shift the burden entirely onto copyright owners to monitor the YouTube site on a daily or hourly basis to detect infringing videos and send notices to YouTube demanding that it "take down" the infringing works. … And even after it receives a notice from a copyright owner, in many instances the very same infringing video remains on YouTube because it was uploaded by at least one other user, or appears on YouTube again within hours of its removal." Complaint, *Viacom Int'l Inc. et al. v. YouTube, Inc. et al,* Case No. 07-CV-2103 (S.D.N.Y. 2007) at 3-4.

[128] "*The 5 Secrets of YouTube's Success*," WIRED 18.04 (April 2010) at 96, *available at* http://www.wired.com/magazine/2010/03/ff_youtube_5secrets/all/1.

[129] *Id*. at 95.

[130] *Id*. at 96.

[131] M. Helft, "*Viacom Says YouTube Ignored Copyrights*," THE NEW YORK TIMES (March 18, 2010), http://www.nytimes.com/2010/03/19/technology/19youtube.html. *See also* K. Hormann, Comment, *The Death of the DMCA? How Viacom v. YouTube May Define the Future of Digital Content*, 46 HOUSTON L. REV. 1345, 1373 (2009) (arguing that expensive filtering technologies are a barrier to entry by other content sharing sites offered by small technology startups, and are contrary to the purposes of the DMCA).

However, despite these advances, *Viacom v. YouTube* continues because copyright holders remain concerned about loss of control of their products in digital form.[132] The ultimate outcome of this case will have a significant defining impact on the rights of copyright holders, online service providers and consumers as more content appears online.

Other DMCA Provisions

The DMCA separately criminalizes the production and dissemination of technology and devices to circumvent digital rights management (DRM) protections for copyrighted works, the so-called "anti-circumvention provisions."[133] The DMCA also contains other miscellaneous clarifications and new provisions not related to cyberspace law.

[132] See M. Helft, *supra.*

[133] 17 U.S.C. §§ 1201-1205.

THE COMMUNICATIONS DECENCY ACT

Andrew B. Serwin

Overview

The Communications Decency Act (CDA)[134] is a federal law that provides civil and criminal immunity in certain cases for statements that are made on the Internet. The CDA also can have impact on privacy and information security issues. Typically, CDA issues arise in situations where individuals post private or defamatory information on the Internet. In some cases, this is done anonymously. In other cases, it is done with attribution. While the CDA affects the liability of the website, or service provider, it does not impact the liability of the author of the statements.

The CDA was passed by Congress in response to a state court decision in New York, *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[135] which held an Internet Service Provider liable for defamation due to message placed upon a message board it ran. Indeed, the basis of that court's ruling was that Prodigy exercised editorial control over the messages because it selectively deleted certain messages, and not others, and therefore it could be liable for deleting some messages, but not others. The Ninth Circuit in a recent CDA case summarized the concerns of Congress as follows:

> In passing section 230, Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they did not edit or delete. In other words, Congress sought to immunize the removal of user-generated content, not the creation of content: "[S]ection [230] provides 'Good Samaritan' protections from civil liability for providers . . . of an interactive computer service for actions to restrict. . . access to objectionable online material. One of the specific purposes of this section is to overrule Stratton-Oakmont [sic] v. Prodigy and any other similar decisions which have treated such providers . . . as publishers or speakers of content that is not their own because they have restricted access to objectionable material." H.R.Rep. No. 104-458 (1996) (Conf.Rep.), as reprinted in 1996 U.S.C.C.A.N. 10 (internal citations omitted) (emphasis in original).[136]

---

[134] 47 U.S.C. §230.

[135] 1995 WL 323710 (N.Y. Sup 1995).

[136] Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157 (9th Cir. 2008).

The concern that led Congress to enact the CDA was the underlying belief that, at least at that time, that the Internet was so delicate that it could be destroyed by the heavy-handed regulation of legislatures and courts, particularly if the courts imposed liability on a service provider for failing to review each posting. This thinking underlies the CDA, the Internet tax debate, Net Neutrality, as well as many other issues.[137] Thus, when one examines the CDA, as well as the court decisions interpreting it, it is helpful to realize that the goal was to promote the growth of the Internet by limiting the liability of Internet Service Providers, also known under the CDA as "interactive computer services" for publishing statements authored by third-parties.

The CDA and Immunity for Publishers

While there are other theories that are litigated in Internet litigation, the CDA most commonly becomes an issue in defamation cases and one of the key factors in defamation lawsuits is whether the defendant is a "publisher" or "speaker" of a false statement. The CDA limits liability by stating that neither providers, nor users, of an interactive computer service will be treated as a publisher or speaker of information that is provided by another information content provider.[138] This effectively eliminates liability for these individuals and entities. This is a much different conclusion than would be reached in the case of print, or other forms of publications, since typically any person who repeats a defamatory statement is considered a publisher. Thus, third-parties who publish the statements of others on the Internet enjoy broader immunity than traditional publishers do.

The CDA also bars liability for any provider or user of an interactive computer service related to: (1) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (2) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described above.[139] The purpose of this exception is to permit ISPs and other users to remove potentially offensive material without facing liability from the person who posts it, or from other users who might claim that the failure to remove the material in a more expeditious manner creates liability for the service provider.

Courts have typically had difficulty applying the CDA, particularly where there is some editing performed by the service provider, or the operation of the website influences the

---

[137] For a more detailed discussion of the CDA, as well as privacy and Internet issues generally, please *see* Andrew Serwin, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE, (West 2009).

[138] 47 U.S.C.A. § 230.

[139] 47 U.S.C.A. § 230(c)(2).

content. In some cases service providers will edit material generated by a third-party before it is posted. Some courts have concluded that the CDA provides immunity for service providers even where they have taken on traditional editorial functions, including deciding whether to publish, withdraw, postpone or alter content.

This is a difficult line to draw and some courts have reached opposite conclusions. For example, certain Courts have not applied the CDA's grant of immunity when the service provider contributes to the content. In light of these cases, certain courts have found the CDA inapplicable where the construction and operation of the website have some influence on the content that is posted. However, other courts have reached different conclusions where a website provided multiple-choice questions and a series of essay questions that shaped the eventual content. Despite the impact of the website on the content, in one case the CDA's grant of immunity was found to apply, even for state law claims of invasion of privacy.

Another common context for CDA issues to arise is in the "gripe site" context. There are certain websites that exist to give individuals the ability to post statements regarding their experiences with certain companies or industries. Certain "gripe sites," in particular, consumer complaint forums, have been disqualified from CDA immunity if they exercise organizational control, added descriptive headings and gave instructions to specific users about what type of content to include. This issue has also been addressed in the case of companies that characterize certain Internet conduct, including companies that create anti-spyware products. Despite the inconsistent results, generally speaking, if the company does not contribute to the content, or create the description of certain programs, the CDA will apply.[140]

CDA Immunity for Criminal Acts and Civil Claims Beyond Defamation

While the CDA is a law targeted towards defamation liability, the scope of immunity is quite broad. In what appears to be a case of first impression, the District Court for the Eastern District of Pennsylvania addressed whether the CDA provided immunity for criminal liability. In *VoiceNet Medications Inc. v. Corbett*,[141] a news reader and Internet Service Provider sued certain government officials for violation of 42 U.S.C. § 1983, based on the immunity afforded them under the CDA and other laws. In this case law enforcement seized the plaintiffs' servers based on the allegation that child pornography was contained on the servers. The plaintiffs argued they were immune from prosecution under the CDA as an interactive service provider and thus the seizure was improper. The Court held that the CDA did provide immunity from criminal liability for service providers.

---

[140] *See, e.g. MCW, Inc. v. Badbusinessbureau.com, L.L.C.*, 2004-1 Trade Cas. (CCH) P 74391, 2004 WL 833595 (N.D. Tex. 2004).

[141] 2006 WL 2506318 (E.D. Pa. 2006).

Additionally, as is shown by the case of *Beyond Systems, Inc. v. Keynetics, Inc.*,[142] the immunity afforded service providers in the civil context extends to negligence, state law unfair competition, tortious interference with prospective economic advantage, claims under Title II of the Civil Rights Act of 1964 and breach of contract claims.

The CDA and Employers

In contrast to other state courts, California courts have concluded that an employer can be an interactive service provider, and hence immune under the CDA, for the acts of its employees if the employee uses the employer's computer system to make threats to others.[143]

Legislative Issues and the CDA

California law contains a number of restrictions on Internet conduct, including restrictions on the publication of certain information on the Internet. As an example, California Government Code § 6254.21 restricts the publication by a state or local agency in California of the home address or telephone number of any elected or appointed official on the Internet without first obtaining the written permission of that individual, and, among other restrictions, also precludes the person to knowingly post the home address or telephone number of any elected or appointed official, or of the official's residing spouse or child on the Internet knowing that person is an elected or appointed official if he intends to cause imminent great bodily harm that is likely to occur, or if he threatens to cause imminent great bodily harm to that individual.[144] Violation of this law gives rise to a number of remedies, including criminal liability, but interactive service providers and access software providers are specifically exempted from liability under this law unless the service or provider intends to abet or cause imminent great bodily harm that is likely to occur or threatens to cause imminent great bodily harm to an elected or appointed official.[145]

While this law appears to account for the impact of the CDA, care must be taken when laws are enacted to ensure that they do not attempt to create liability that cannot exist under the CDA.

[142] 422 F. Supp. 2d 523 (D. Md. 2006).
[143] *Delfino* v. *Agilent Technologies, Inc.*, 145 Cal. App. 4th 790 (2006).
[144] Cal. Gov't Code § 6254.21(b).
[145] Cal. Gov't. Code § 6254.21(e).

DOMAIN DISPUTES

Jefferson F. Scher

Overview

Amazon.com. GoDaddy.com. Pets.com. Some of the internet's best known business names and brands have been *domain names*. Conversely, many of the world's most recognized companies and products can be found on the internet by adding ".com" to the end of their business name (e.g., Apple.com) or trademark (e.g., BlackBerry.com).

As a technical matter, there is no necessary connection between web addresses and trademarks. Nevertheless, federal and state law, and domain registration agreements, recognize that consumers may be confused or deceived by the use of established brands or personal names as domain names. They also recognize, to varying degrees, that even a year-to-year registration of a domain name gives rise to some property-like rights that its owner can exercise to protect its ability to continue use of the domain name.

Key Points:

- Domain Names Similar to Trademarks are Subject to Challenge:
  - When used in connection with goods or services, under federal, state, and common law trademark, unfair competition, and anti-dilution law;
  - When used or registered in "bad faith," under the Anti-Cybersquatting Consumer Protection Act;[146] or
  - When used and registered in "bad faith," for certain domains, through a private arbitration proceeding under the Uniform Domain Name Dispute Resolution Policy (UDRP)[147] (reviewable *de novo* in District Court).
- Domain Names Consisting of Personal Names are Subject to Challenge:
  - When registered for resale, under the Anti-Cybersquatting Consumer Protection Act (living persons only); or
  - When used or registered in "bad faith," under California Bus. & Prof. Code § 17525 et seq. (living persons and deceased personalities).
- Both trademark claims and the assessment of "bad faith" are subject to competing intellectual property rights and free speech rights, making individual determinations unusually unpredictable.

[146] 15 U.S.C. § 1125(d).
[147] See http://www.icann.org/urdp.

Discussion

Background: The Domain Name System

An individual or company, the *registrant*, applies for a domain name through a *registrar*, such as Network Solutions or GoDaddy. This generally requires that they enter into a contract governing the conditions and duration of use of the domain name with the registrar. The registrar will secure registration with the appropriate *registry* for the corresponding top level domain ("TLD," e.g., ".com" in "newco.com"). The customer may purchase other services from the registrar, such as email and web hosting services, or may secure those services elsewhere. Either way, the registrar is responsible for providing address information that allows internet users to find the correct servers.

All communications on the internet are routed by numeric addresses known as "internet protocol" or IP addresses. The domain name system ("DNS") provides for a transparent conversion between a memorable web address such as "www.facebook.com" and the easily forgettable (and mistyped) IP address 69.63.180.14. When your browser requests a page from "www.latimes.com" or your mail server wishes to send a message to "feedback@sfgate.com," one or more DNS servers provide the necessary numeric address to fulfill that request.

There is no single DNS server that can resolve all of the world's domain names to their corresponding IP addresses. Instead, the information is divided among numerous servers, each of which is considered authoritative for certain information. Consider the case of "www.carrferrell.com." The registry operator for the .com top level domain refers users to the DNS servers (also known as name servers) maintained by the registrar responsible for carrferrell.com, which directs users to the DNS servers for the web hosting company, which ultimately supplies the actual IP address for www.carrferrell.com.

In addition to twenty-one "generic" TLDs ("gTLDs"), such as .com, .org, and .gov, there are individual national TLDs (country-code TLDs, or "ccTLDs"), including .us, .uk, and .jp. Nations administer ccTLDs under their own policies, and while most require some geographic or legal nexus, some (such as .tv) are open to all applicants. The Internet Corporation for Assigned Names and Numbers ("ICANN"), a not-for-profit corporation which oversees the operation of DNS, plans to allow for a multitude of new gTLDs. These would be proposed by and awarded to potential registry operators not deterred by the $185,000 application fee.

Domain Names and Trademarks

Domain names may act as identifiers for web businesses, but they differ fundamentally from trademarks. Domain names are globally unique, allocation is based on a first-

come, first-served principle regardless of prior similar domain name registrations, and ownership can be maintained through payment of an annual fee. By contrast, multiple companies can use the same trademark without confusion for different product or in different geographic markets, their rights arise from use and from registration subject to prior similar marks, and rights may be abandoned through non-use even if registration is nominally maintained.

To reconcile these differences, the principles of trademark, unfair competition, and anti-dilution law are applied on a case-by case basis, after domain registration, to determine whether a given registrant has infringed the rights of a given trademark holder, and therefore must relinquish ownership of the domain to that mark holder. Where the usage does not give rise to confusion, or is not diluting, the mark holder still may prevail on the grounds that the domain was registered in bad faith.

Trademark-based challenges to domains arise in a variety of contexts. In some cases, the registrant is another, coexisting trademark user, with an arguably equal right to the domain. At the other extreme, the domain may be used by nefarious competitors to divert customers, or by cybercriminals to commit fraud including "phishing" scams. More ambiguous cases have involved unauthorized use by resellers, and use by "domainers" to earn pay-per-click advertising revenues from confused web users. Finally, some cases have involved unofficial "fan" sites and "protest" sites, operated by customers or community members, which raise questions about the balance between protection for trademarks and protected speech. The term "cybersquatting" now transcends the practice of warehousing a domain for future use or resale, and is applied to a wide variety of practices deemed to constitute bad faith which sometimes are termed "cyberpiracy."

Likelihood of Confusion. The federal Lanham Act sections 32 and 43(a)[148] provide remedies for the infringement of registered and unregistered marks. California law provides similar remedies under Business & Professions Code § 14245. Relief will be granted if the domain name creates a *likelihood of confusion* as to the source, sponsorship, or affiliation of the registrant's goods and services. As in offline cases, courts apply the traditional multi-factor test, considering the similarity of the asserted mark and domain name in appearance, sound and meaning; the parties' respective goods, services, and marketing channels; the distinctiveness and renown of the mark; the nature and sophistication of the target customers; and other factors.[149] In many cases, this analysis may fail to establish infringement, either because there is no active website or because the site's contents are unrelated. Further, even if the analysis establishes infringement, the defendants may successfully invoke a First Amendment defense nullifying any

[148] 15 U.S.C. §§ 1114 and 1125(a).

[149] See, e.g., Internet Specialties West, Inc. v Milon-Digiorgio Enterprises, Inc., 559 F.3d 985 (9th Cir. 2009).

infringement. Accordingly, trademark owners have reached for many other theories of liability to combat cybersquatting.

Initial Interest Confusion. The Court of Appeals for the Ninth Circuit has been especially active in applying the theory of "initial interest confusion" in internet cases. This theory holds that even if a user is no longer confused as to the source of a website once he or she views the page, the *initial* confusion that led him or her there may be actionable. However, in order to obtain relief, the defendant's site must have the potential for diverting business from the trademark holder's site due to a similarity in goods and services.[150] There is no *per se* rule that users expecting to find Company X at "companyx.com" have suffered initial interest confusion by making that guess.[151]

Bad Faith Registration or Use. The Anti-Cybersquatting Consumer Protection Act ("ACPA")[152] provides a cause of action applicable to a wide variety of domain names deemed to have been registered or used in bad faith. The Uniform Domain Name Dispute Resolution Policy ("UDRP"), which is incorporated into most domain registration agreements under popular gTLDs, requires the registrant to submit to arbitration of trademark-related challenges to the domain. Arbitration is at the election of the mark holder, who may choose instead to proceed in court.

These two legal regimes impose considerably different requirements on mark holders:

ACPA	**UDRP**
(1) Domain identical or confusingly similar to (or dilutive of) a mark distinctive (famous) at the time the domain was registered; (2) Registrant registered, trafficked in, *or* used the domain with a bad faith intent to profit from the mark	(1) Domain identical or confusingly similar to complainant's mark; (2) Registrant registered *and* used the domain in bad faith; and (3) Registrant has no rights or legitimate interests in the domain
Circumstances tending to show bad faith (nonexclusive): (V) Intent to divert consumers to a site that could damage goodwill, by creating source or sponsorship confusion either for commercial gain, or with the intent to tarnish/disparage	Circumstances tending to show bad faith (nonexclusive): (i) registered or acquired the domain primarily for the purpose of selling/renting/transferring it to complainant or its competitor for valuable consideration in excess of registrant's out-of-pocket costs directly

[150] *Interstellar Starship Services Inc. v. Epix Inc.*, 304 F.3d 936, 942-43, 64 U.S.P.Q.2d 1514 (9th Cir. 2002) (parties offered different services to different target markets; EPIX is not highly distinctive).

[151] *See id.* at 945.

[152] 15 U.S.C. § 1125(d).

ACPA	UDRP
the mark; (VI) Offer to transfer domain for financial gain without making (or having had the intent to make) legitimate commercial use – or – prior conduct indicating a pattern of such conduct; (VII) Providing "material and misleading" false contact information in registering the domain, or intentionally failing to keep it accurate – or – prior conduct indicating a pattern of such conduct; (VIII) Pattern of intentional registration or acquisition of domains confusingly similar to (dilutive of) the distinctive (famous) marks of others — regardless of goods/services	related to the domain; (ii) registered the domain to prevent the TM owner from reflecting the mark in a corresponding domain, *provided* registrant has engaged in a pattern of such conduct; (iii) registered the domain primarily to disrupt the business of a competitor; (iv) by using the domain, registrant has intentionally attempted to attract users to its website/other on-line location, for commercial gain, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of its website/location or of a product or service on its website/location
Circumstances tending to show no bad faith, to be balanced with other facts in assessing overall conclusion on bad faith: (I) TM or other IP rights in the domain (II) Domain is registrant's legal name or name by which he is commonly known (III) Prior use of the domain for legitimate commercial activities (IV) Noncommercial or fair use of the mark at a site hosted under the domain name	Circumstances tending to show rights or legitimate interests (complainant must "prove a negative"): (i) before any notice of the dispute, registrant used or made demonstrable preparations to use, the domain in connection with a bona fide offering of goods or services; (ii) registrant has been commonly known by the domain name, even if it has acquired no trademark or service mark rights; (iii) registrant is making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.
Suit may be brought where there is	Arbitration may be filed with one of

ACPA	UDRP
personal jurisdiction. If personal jurisdiction cannot be obtained, then suit may be brought against the domain *in rem* at the site of the registry (for .com domains, Northern Virginia).	three approved providers. The jurisdiction for any appeal by the registrant is either the location of the registrant or of the registry, as elected in the complaint by the complainant.
Relief may include transfer of the domain, damages (actual, treble, or statutory), costs, and fees	Relief may include transfer of the domain

Dilution. The Federal Trademark Dilution Act ("FTDA")[153] provides remedies for the dilution of famous marks. California law provides similar remedies under Business & Professions Code § 14247. Before the passage of the ACPA, the broad language of the FTDA provided a powerful weapon against cybersquatters; courts almost automatically ordered the transfer of a domain identical to a famous mark. However, with recent revisions to the FTDA that raised the burden of proof, and the ready availability of relief based on the registrant's bad faith, the FTDA has become much less important in domain disputes. [154]

Reverse Domain Name Hijacking. Some mark holders have initiated domain name disputes with an eye toward wresting a domain away from a registrant equally entitled to use it, a practice dubbed "reverse domain name hijacking." Under the UDRP Rules, arbitration awards may declare a complaint filed in bad faith to constitute an abuse of the process, but no costs or fees may be awarded against the complainant. Under the ACPA, an objectively meritless cybersquatting claim may satisfy the Lanham Act's "exceptional case" threshold for a fee awards to the registrant.

A more troubling motivation for litigation may be to shut down "protest" websites and other protected speech. While it is important to protect the public from confusion about the sponsorship of such sites, where that clearly is not an issue, tribunals often may be unable to compensate the registrant for the costs of litigation.

Domain Names and Personal Names

The names of individuals, particularly athletes, musicians, and other celebrities, have been popular among cybersquatters and loyal fans alike. Because these names may not yet be protected as trademarks at the time of registration, both Congress and the California legislature have enacted provisions protecting personal names. Both statutes

[153] 15 U.S.C. § 1125(c).

[154] *See* 4 J.T. McCarthy, *McCarthy on Trademarks* §24:71 (2008).

create exemptions for the names of literary characters, to avoid any conflict with copyright law.

The scope of protection under the ACPA is somewhat narrow: relief is available only when a domain constitutes the name of a living individual and was registered with the specific intent to resell the domain.[155] By contrast, California law protects both living individuals and deceased personalities, and applies a flexible balancing test for bad faith similar to the test applied to trademark claims under the ACPA.[156]

Domain Names as Property

Courts have differed over whether a registrant has as a property right in a domain name or merely a covenant to provide DNS services for the term of the registration agreement. There can be little doubt that domains can accumulate good will and often have substantial resale value. Accordingly, a registrant's interest typically will be protected against wrongful conversion.

[155] 15 U.S.C. § 1129.

[156] Cal. Bus. & Prof. Code § 17525 et seq.

KEYWORD SEARCH

Bennet Kelley

Overview

Greek mythology teaches us that in the beginning there was only confusion and chaos. That is a good starting point for understanding the current state of the law with respect to an advertiser's use of competitors' trademarks in keyword search ads. Courts have stumbled over two key points: 1) whether bidding on a competitor's trademark is a "use in commerce" so as to trigger federal trademark laws; and 2) if the mere use of the competitor's trademark as a search term alone (as opposed to using it in the displayed text) results in liability.

Discussion

Use in Commerce

Since the federal Lanham Trademark Act[157] is derived from Congress' authority to regulate interstate commerce, the threshold element of any Lanham Act claim is that it involves a "use in commerce" of the disputed trademark. This would appear to be a no-brainer since we all know that keyword search advertising is big business, with revenue exceeding $50 million per day worldwide in 2007. In this context, most courts have had little difficulty in concluding that the purchase of keyword search advertisements satisfies the threshold of a use in commerce.

The Second Circuit Court of Appeals (which covers Connecticut, New York and Vermont) however, has taken a more literal interpretation of the statute, finding that there is no use in commerce in keyword search terms since the trademark is neither placed "on any product, good or service," nor is the use of the mark visible to the consumer.

Establishing Liability

Establishing "use in commerce" merely gets you in the courthouse door, as a plaintiff still must prove use of a trademark by a party in a manner that "is likely to cause confusion, or to cause mistake, or to deceive [a consumer] as to the affiliation... origin, sponsorship, or approval" of such goods or services. Since this is inherently a subjective test, courts have created a series of factors to be weighed in evaluating whether there is a likelihood of confusion that includes the strength of the trademark, the degree of similarity between the marks at issue, the competitive proximity of the goods or

[157] 15 U.S.C. §§ 1051-1127.

services involved, evidence of actual confusion, the defendant's intent and the sophistication of the buyers for the goods or services involved.

Unfortunately for online advertisers, the real likelihood of confusion occurs when courts attempt to apply this standard in the keyword search context; they have struggled to find appropriate offline analogies to guide their decisions--and this may be the problem.

The lead case on this issue was decided in 1999 at a time when less than half of U.S. households had Internet access. In *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*,[158] the Ninth Circuit compared West Coast Video's use of Brookfield's "MovieBuff" trademark in meta tags to posting a sign on the highway diverting would-be Brookfield consumers to the wrong exit. "Unable to locate [Brookfield], but seeing the [West Coast Video] store right by the highway entrance, they may simply rent there" instead of returning to the highway.

The court explained that while the consumer knows they are patronizing West Coast Video and not Brookfield, "there is nevertheless initial interest confusion in the sense that, by using [the trademark] to divert people looking for 'MovieBuff' to its website, West Coast improperly benefits from the goodwill that Brookfield developed in its mark." This "initial interest confusion," according to Professor McCarthy, the author of the leading treatise on trademark law, is simply a cyber-variation of "bait and switch." The fact that any confusion is later dispelled does not eliminate the infringement that has already occurred.

"The initial interest confusion doctrine is a mess." That is how one public interest group opened its argument in briefing the issue--and with good reason. As the doctrine has been adopted in several circuits, it has been applied in an inconsistent manner with no clear definition of its elements, the factors to be considered or even who bears the burden of proof (one court turned the Lanham Act on its head and placed the burden on the advertiser to disprove the absence of initial confusion). More fundamentally, there is disagreement as to whether the doctrine is one of the many factors to be considered in evaluating the likelihood of confusion or a separate standard in itself--a point on which the Ninth Circuit has reversed itself on three occasions. How can an advertiser effectively defend against such a claim when it essentially is a moving target?

A Battle of Analogies

A number of courts have disagreed with the *Brookfield* court's dim view of Internet users, noting that such users are unlikely to be discouraged by landing on the wrong website when all that is required to remedy the situation is the touch of the back key. In

[158] 174 F.3d 1036 (9th Cir. 1999).

a battle of analogies, doctrine opponents argue that far from being a detour from a cyber highway, jumping from a website back to a search engine results page is merely a lane change. Doctrine opponents note that courts following Brookfield fail to recognize that a consumer typing in a trademarked term not only expects to see results involving other companies, but that it may, in fact, be their objective. Thus, instead of a bait and switch, displaying competing offers in response to a search using a trademarked term is equivalent to a supermarket placing competing brands adjacent to each other in the same aisle.

Opponents also argue that the doctrine loses sight of the purpose of trademark law: to protect consumers from being deceived and businesses from unfair competition. While the Lanham Act's goal is to foster legitimate competition, the mis-application of this doctrine stifles competition by limiting competitive advertising directed to search engine shoppers.

Although there is no clarity among courts applying the initial interest confusion doctrine, there is a clear line being drawn in jurisdictions rejecting the doctrine. Courts in these jurisdictions have held that an advertiser may freely bid on its competitors' trademarks as search terms without liability so long as the marks are not used in the display ad itself. Using a trademark in the search ad is problematic if not clearly used in a comparative setting; it is very difficult to include disclaimers in an ad that is limited to 70 characters.

Beyond *Brookfield*

In Greek mythology, chaos gave way to the birth of Titans. With U.S. search marketing accounting for $8.8 billion in revenue in 2007, it is clear a titan is emerging, but its continued growth may be hindered by a prolonged state of chaos over keyword search liability. It is time to recognize that *Brookfield* was decided in a different age. The Internet is no longer in its infancy and, despite the intervening dot-com crash, has enjoyed dramatic growth as evidenced by increases in U.S. Internet usage (75 percent), e-commerce sales (400-plus percent), domestic search revenue (10,000-plus percent) and the size of the Internet (it's doubled five times over).

Now that we are firmly planted in the digital age, courts should revisit the question of initial interest confusion and develop a solution that is both consistent with the Lanham Act and based on Internet realities--instead of tortured offline analogies.

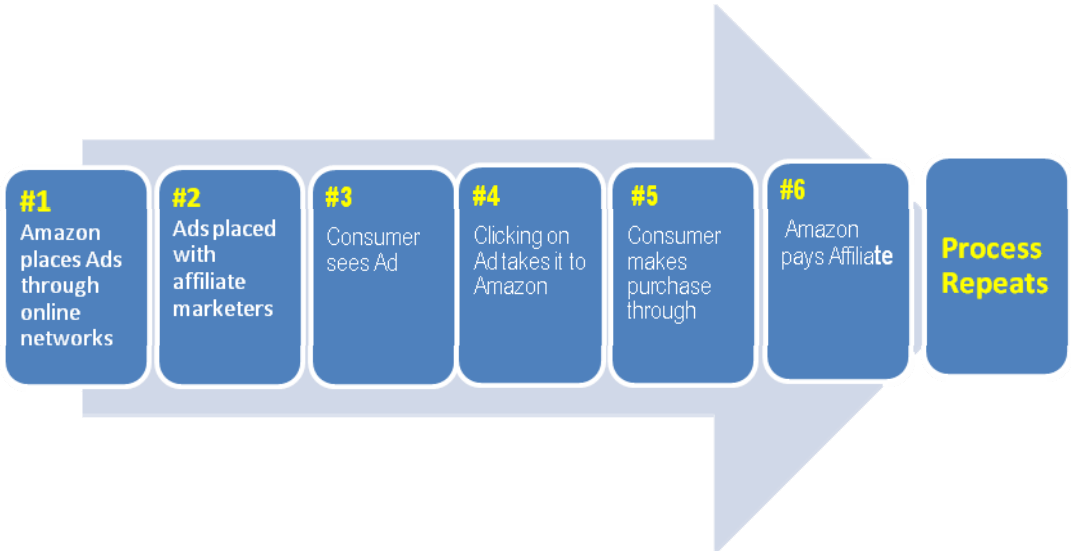
"Amazon Tax"

Bennet Kelley

Overview

The Due Process and Commerce Clauses of the Constitution limit a state from imposing tax liability or collection responsibilities on a business concern unless there is a substantial nexus or in-state contact established with the state.[159] The "Amazon Tax" is not a tax per se but rather an effort by states to redefine nexus in such a way as to reach out of state online merchants who pay commissions to third parties located within the state. It has been enacted in New York, Rhode Island and North Carolina and passed in California but was vetoed by Governor Schwarzenegger in 2009.

The Amazon Tax is also often referred to as an "Affiliate Tax" or "Advertising Tax" because the obligation of an online merchant to pay the tax is only triggered if in-state affiliate marketers who the merchant advertises with receive commissions above a threshold level. Affiliate marketers are not affiliates of an online merchant in the legal sense but rather third party websites, marketers and intermediary networks who drive traffic to the merchant site through advertisements on the affiliate sites or networks. Affiliates are paid either on a Cost per Action (CPA), Cost per Click (CPC) or Cost per Thousand (CPM) basis. *See* Affiliate Marketing Cycle below.



The industry has a strong presence in California, with 22 of the top 25 ad networks and 10 of the top affiliate networks being based or having an office in California.[160]

---

[159] *Quill Corp.* v. *North Dakota*, 504 U.S. 298 (1992)

[160] Based on ComScore April 2009 ranking of Ad Networks and Website Magazine's April 2009 ranking of Affiliate Networks.

Discussion

Constitutional Limitations

In *Quill Corp. v. North Dakota*[161], the Supreme Court reversed North Dakota's attempt to tax an out of state mail order company with no in state presence, stressing the value of a bright line test for taxing out of state entities.

> Undue burdens on interstate commerce may be avoided not only by a case by case evaluation of the actual burdens imposed by particular regulations or taxes, but also, in some situations, by the demarcation of a discrete realm of commercial activity that is free from interstate taxation. . . . Such a rule firmly establishes the boundaries of legitimate state authority to impose a duty to collect sales and use taxes and reduces litigation concerning those taxes. . . . Moreover, a bright line rule in the area of sales and use taxes also encourages settled expectations and, in doing so, fosters investment by businesses and individuals.

It is permissible, however, for states to tax online sales for out of state entities where the entity has either an in-state presence or an agent in-state.[162]

New York Law

The so-call Amazon tax arises from the New York's decision to extend the definition of an in-state agent to include a resident who

> for a commission or other consideration . . . refers potential customers, whether by a link on an internet website or otherwise, to the seller, if the cumulative gross receipts from sales by the seller to customers in the state who are referred to the seller by all residents with this type of an agreement with the seller is in excess of [$10,000].[163]

This definition may be rebutted by proof that the resident with whom the seller has an agreement did not engage in any solicitation in the state on behalf of the seller that would satisfy the nexus requirement of the United States constitution; by paying in

---

[161] 504 U.S. at 315-316.

[162] *Borders Online, LLC* v. *State Bd. of Equalization*, 129 Cal.App.4th 1179, 29 Cal.Rptr.3d 176 (2005); *contra*, *St. Tammany Parish Tax Collector* v. *Barnesandnoble.com*, 481 F. Supp. 2d 575, 582 (E.D. La. 2007).

[163] New York Tax Code § 1101(b)(8)(vi).

state marketers on some basis other than commission or by including and enforcing a prohibition on New York marketing in marketer contracts.[164]

The New York law became known as the Amazon tax because it was directed at large online retailers such as Amazon.com that only collects sales tax in its home state of Washington. In its first two years, New York's Amazon tax exceeded expectations and raised over $100 million in new revenue.[165] The Amazon tax, however, has a steep price for some, since Overstock.com and many other online retailers simply terminated their New York marketers to avoid having to comply with the New York law.[166]

Amazon.com and Overstock.com challenged the constitutionality of the statute, but their complaint was dismissed by the trial level judge since the New York law:

> requires a substantial nexus between an out-of-state seller and New York through a contract to pay commissions for referrals with a New York resident along with realization of more than $10,000 of revenue from New York sales earned through the arrangement. The neutral statute simply obligates out-of-state sellers to shoulder their fair share of the tax collection burden when using New Yorkers to earn profit from other New Yorkers.[167]

The ruling is on appeal and a decision from the New York Court of Appeal is expected in early 2010.

In 2009, Rhode Island and North Carolina adopted similar provisions with Amazon.com and other online retailers terminating all in state marketers immediately thereafter.[168] The growing popularity of the Amazon tax has been

---

[164] "New Presumption Applicable to Definition of Sales Tax Vendor," New York State Department of Taxation and Finance, Office of Tax Policy Analysis, Taxpayer Guidance Division, TSB-M-08(3)S (May 8, 2008); "Additional Information on How Sellers May Rebut the New Presumption Applicable to the Definition of Sales Tax Vendor as Described in TSB-M-08(3)S", New York State Department of Taxation and Finance, Office of Tax Policy Analysis, Taxpayer Guidance Division, TSB-M-08(3.1)S (June 30, 2008)

[165] Michael Mazerov, "New York's 'Amazon Law': An Important Tool for Collecting Taxes Owed on Internet Purchases," Center for Budget and Policy Priorities (July 23, 2009).

[166] See "Merchants Removing New York Affiliates," NYAffiliates.com.

[167] *Amazon.com LLC v. New York State Dept. of Taxation & Finance*, 23 Misc.3d 418, 877 N.Y.S.2d 842 (N.Y. Supreme Ct., N.Y. County, 2009)

[168] Lauren Brown, "Amazon Tax: 2009 Update," Inside ALEC (Sept-Oct 2009) at 16.

condemned by public interest groups on the right and hailed by those on the left.[169]

Amazon Tax Migrates to California

Like the Dodgers and Giants a half-century ago, it was only a matter of time before the Amazon tax reached California. In 2009, Assemblywoman Nancy Skinner introduced AB 178 which was a carbon copy of the New York law. Assemblywoman Skinner stressed that the legislation (i) is not a tax but merely imposes an obligation to collect an existing tax liability since consumers have a duty to pay sales tax on out of state online purchases; and (ii) prevents out of state e-commerce sites from having an unfair competitive advantage over in-state businesses who must collect sales tax.[170] The Board of Equalization estimated that the bill would yield $149.5 million annually.[171]

Opponents of the legislation said that the legislation could cost 16,000 jobs and $1 billion in revenue due to termination of in-state affiliate marketers. After the proposal was included in a budget package approved by both houses, Overstock.com terminated all of its California affiliates -- a fact cited by Governor Schwarzenegger in his budget veto.[172] Having failed passage in the Assembly before January 31, 2010, the bill now is inactive, filed with the Chief Clerk of the Assembly pursuant to Joint Rule 56.

---

[169] Compare Joseph Henchman and Justin Burrows, "Amazon Tax" Unconstitutional and Unwise," Fiscal Fact (September 15, 2009) and Michael Mazerov, "New York's 'Amazon Law': An Important Tool for Collecting Taxes Owed on Internet Purchases," Center for Budget and Policy Priorities (July 23, 2009).

[170] "Assemblymember Nancy Skinner Announces Legislation to Close Tax Loophole and Bring Much Needed Revenue to California" (Feb. 2, 2009).

[171] Assembly Committee on Revenue and Taxation Staff Analysis of AB 178 (April 27, 2009).

[172] "Governor Schwarzenegger Remains Committed to No New Taxes, Announces Overstock.com Will Continue to do Business in California," (July 1, 2009).

SOCIAL NETWORKING

AN OVERVIEW OF SOCIAL NETWORKING

Andrew Serwin

Social networking is a service offered predominantly through the Internet that permits people to connect with friends and form relationships with new individuals. The power of social networking is based on people disclosing and sharing information with people they know, and in some cases with people they do not. Sharing of information with unknown people has the possibility of permitting people to form these new relationships, but also presents the greatest risks to privacy and safety in that the use of social networking can result in sensitive information being disclosed beyond the social networking service (including to employers). There are also physical safety concerns to consider, particularly in the case of children.

Social Networking and the Impact of Internet and Electronic Privacy Laws

Two of the main areas of law that impact social networking sites are internet privacy and electronic communications privacy laws. California is one of the few states that has regulated Internet privacy via the Online Privacy Protection Act of 2003.[173] It requires businesses to disclose their privacy practices to California consumers. The stated goal of this law is to regulate the security and confidentiality of the consumers' personally identifiable information obtained by persons and entities engaged in online business transactions. A website owner must conspicuously display a privacy policy if the site collects personally identifiable information. The privacy policy must disclose several key items, including the categories of personally identifiable information that the operator collects through the website, provide a description of the process the operator uses, if any, for consumers to review and request changes to any of his or her personally identifiable information that is collected through the website, describe the process that is used to notify consumers who use or visit the site of material changes to the privacy policy, and identify its effective date. There are also specific requirements regarding where the policy is posted as well as formatting requirements. Several other states have regulated Internet privacy, but California's law provides the most comprehensive protections.

Given the prevalence of chat and email capability on social networking sites, laws that protect the privacy of electronic communications should also be noted. At the federal level, the Electronic Communications Privacy Act, or "ECPA" prohibits the disclosure or monitoring of electronic communications in certain circumstances. There are two portions of the ECPA—the Wiretap Act and the Stored Communications Act.[174] The

[173] Cal. Bus. & Prof. Code § 22575 *et seq.*

[174] See 18 U.S.C.A. § 2510, *et seq.* and 18 U.S.C.A. § 2701, *et seq.*

Wiretap Act applies to communications while they are in transit, and the Stored Communications Act generally applies to communications that have reached their destination, and are therefore considered to be in storage. The ECPA provides a common national standard of protection for electronic communications, but it is generally not considered to preempt state laws that impose higher burdens. California has enacted the Invasion of Privacy Act, found at California Penal Code § 631 *et seq.* It, like the ECPA, regulates the disclosure of communications, including electronic communications. California law goes beyond the ECPA in several respects, including requiring two party consent for the monitoring or recording of certain confidential communications. In contrast, ECPA permits monitoring or recording of communications with one party's consent. Since social networking sites often permit the transmission of communications, these laws are important to consider.

The CDA and Social Networking

The Communications Decency Act (CDA)[175] is discussed in an article above, but social networking presents some different circumstances that affect the application of the CDA. One issue that has arisen is the scope of CDA immunity where the service provider has served as an intermediary for improper conduct, including issues with minors and other forms of alleged sexual misconduct. Certain plaintiffs have alleged that social networking sites know sexual predators are using their services and therefore CDA immunity does not exist. This argument was recently rejected by the Fifth Circuit when it found that MySpace was immune from claims that it had allegedly failed to implement safety procedures to prevent sexual predators from allegedly misusing MySpace.[176] The Court did not consider the plaintiffs' argument that MySpace lacked immunity under the CDA due to its alleged role in creating the content due to an online questionnaire. However, it should be noted that the Ninth Circuit recently addressed this issue and given the questionnaire as described in the *Doe v. MySpace, Inc.* case, it would appear to fall within the "neutral" category that would still support immunity.

Posting of Information on Social Networking Cites Operating as a Waiver of Privacy

Most states have protected individual privacy via the state constitution, by statute, or common law. California has explicitly protected the right of privacy as a constitutional right.[177] As a result, there are a multitude of cases examining and defining the scope of California residents' privacy rights. California also recognizes a common law right to privacy, but it is recognized that the constitutional right to privacy is broader, and in fact encompasses the common law privacy rights. Privacy rights are not absolute and can be waived by conduct, including disclosure on social networking sites. In *Beye v.*

[175] 47 U.S.C.A. §230.
[176] *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008).
[177] *See* Cal. Const. Art. 1 § 1.

Horizon Blue Cross Blue Shield of New Jersey, the District Court addressed an issue that will likely recur—the impact on a person's privacy of their voluntary disclosure of sensitive information on a social networking site. In this case the court ordered the plaintiffs to produce evidence that was posted on social networking sites, even if it reflected sensitive medical conditions (allegedly eating disorders in this matter), because of the diminished expectation of privacy due to the posting and sharing of the information.[178]

Social Networking and Spam Laws

CAN-SPAM, or Controlling The Assault of Non-Solicited Pornography and Marketing Act of 2003, was passed due to the legislative reaction to certain state email laws, California's in particular.[179] These state laws went far beyond what the federal government was willing to do, so CAN-SPAM was passed with the goal of preempting (in essence nullifying) the troublesome portions of state law. CAN-SPAM was not initially well received, though the criticism seems to have died down in recent times. The main criticism of CAN-SPAM is that it did not explicitly prohibit unsolicited emails. Despite this perceived shortcoming, CAN-SPAM has increased the FTC's ability to stop spam. States at this point seem to be taking a back seat to the FTC on these issues, though state-based email actions still occur. California has enacted a new email law in response to CAN-SPAM. One of the unique features of California's law is that an email must be unsolicited to be actionable, even if the email is deceptive, if the action is brought by an individual. California also regulates commercial emails under Penal Code § 502.

Generally, under California law it is illegal to initiate or advertise in an unsolicited commercial email advertisement from California or advertise in an unsolicited commercial email advertisement sent from California, initiate or advertise in an unsolicited commercial email advertisement to a California electronic mail address, or advertise in an unsolicited commercial email advertisement sent to a California electronic mail address.[180] This law is of import in the social networking arena because many times social networking sites are used improperly by users for commercial purposes. However, while California narrowed the scope of its spam law in response to CAN-SPAM, even California's new formulation of its commercial email laws has encountered preemption problems in the social networking context. In Facebook, Inc. v. Connectu, LLC, the Court rejected an argument that CAN-SPAM only preempted laws that were in effect when it passed in 2003. The Court then assessed whether §§ 17529.4 and 17529.45 were preempted by CAN-SPAM, ultimately concluding that the statutes were preempted.[181]

---

[178] *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, 2:06-cv-05337-FSH-PS (D. N.J. December 14, 2007).

[179] *See* 15 U.S.C.A. 7702, *et seq.*

[180] *See* Cal. Bus. & Prof. Code § 17529.1, *et seq.*

[181] *Facebook, Inc. v. Connectu, LLC*, 489 F.Supp.2d 1087 (N.D.Cal. 2007).

Computer Crime Laws

California Penal Code § 502 regulates unauthorized access to computers and computer networks and it impacts social networking because users' conduct can violate this law if social networking sites are used for improper or illicit purposes. Under California law it is an offense if any person: (1) knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either: (a) devise or execute any scheme or artifice to defraud, deceive, or extort; or (b) wrongfully control or obtain money, property, or data; (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network; (3) Knowingly and without permission uses or causes computer services to be used; (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network; (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network; (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of Section 502; (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network; (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network; or (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.[182]

Cyberstalking

Conduct on social networking sites can also implicate cyberstalking laws.[183] An individual is liable for the tort of stalking in California when the plaintiff proves the defendant engaged in a pattern of conduct the intent of which was to follow, alarm, or harass the plaintiff, that as a result of that pattern of conduct, the plaintiff reasonably feared for his or her safety, or the safety of an immediate family conduct made a credible threat with the intent to place the plaintiff in reasonable fear for his or her safety, or the safety of an immediate family member and, on at least one occasion, the plaintiff clearly and definitively demanded that the defendant cease and abate his or her

[182] Cal. Penal Code § 502.
[183] Cal. Penal Code § 422

pattern of conduct and the defendant persisted in his or her pattern of conduct, or the defendant violated a restraining order. In order to establish the element of intent, the plaintiff is required to support his allegations with independent corroborating evidence.

This law implicates cyberstalking and social networking because the definition of "credible threat" includes threats made via electronic communications. It should be noted that this law does not in any way attempt to impair any constitutionally protected activity, including, but not limited to, speech, protest, and assembly. Any person who commits this tort is liable for damages, including, but not limited to general and special damages, as well as punitive damages. Equitable relief is also permitted. There are also criminal penalties.

SOCIAL NETWORKING SITES AND AGE VERIFICATION ISSUES[184]

Francoise Gilbert[185]

The anonymity and openness of the Internet environment allow anyone to easily register as a user on a site using a different identity than the actual one. As a result, many minors and children have been able to find their way onto social networking sites. In some cases, these minors or children met adults online, the relationship was moved off-line, and prohibited sexual activities ensued. Many children and minors have become the victims of child predators whom they met offline.

Governments and legislators are looking at **age verification** as a way to protect children and minors from inappropriate contacts on the Internet. This article explores some of the issues raised by age verification and looks at the status of laws and government enforcement actions that focus on keeping children and minors out of sites that are not intended for them, or not prepared to handle them.

Background

The case *John Doe v. SexSearch.com*[186] provides an example of encounters that may result where there is no verification of the age or other information provided by a registrant. SexSearch.com is a website offering an online adult dating service which encourages its members to meet and engage in sexual encounters. Members are permitted to provide information for a profile and to upload photographs and video content to their profile.

Shortly after he became a member of SexSearch.com, John Doe located Jane Roe's profile, which provided Jane Roe's birth date, her age (18), and an authentic image of Jane Roe at her then-current age. After chatting online through SexSearch.com, the two decided to schedule a sexual encounter. The meeting went as planned, and the two engaged in consensual sexual relations. However, Jane Roe was actually 14. A few weeks after their encounter, John Doe was arrested and charged with engaging in unlawful sexual conduct with a minor, which exposes him to 15 years in prison, and a classification that might include lifetime registration as a sex offender.[187] In *John Doe v.*

 This article is based on Francoise Gilbert, *Age Verification as a Shield for Minors on the Internet: A Quixotic Search?*, 5 SHIDLER J. L. COM. & TECH. 6 (2008), *available at* http://www.lctjournal.washington.edu/Vol5/a06Gilbert.html (last visited March 9, 2010).

[185] Françoise Gilbert is a principal of the IT Law Group, www.itlawgroup.com, a law firm based in Palo Alto, CA. Her practice focuses on information privacy and security and data governance. She has assisted global and local companies on a wide range of data protection, data governance, and compliance issues. Ms. Gilbert can be reached at: (1) 650-804-1235 or fgilbert@itlawgroup.com

[186] *John Doe* v. *SexSearch.com*, Case. No. 3:07 CV 604, U.S. Dist. Ct ., N. District of Ohio.

[187] Information from Memorandum Opinion and Order, Judge Jack Zouhary, document No. 153 filed August 22, 2007.

SexSearch.com, the plaintiff sued the social networking site for having failed to adequately screen the minor during the registration.

US Legislative Activity

Federal Legislation

The risks to which children and minors are exposed when using social networking sites have prompted legislators to introduce bills aimed at increasing the protection of children and minors. For example, in September 2008, the US President signed into law two bills that address the protection of children online: Senate Bills S. 431 and S. 1738.

Senate Bill S. 431, ***Keeping the Internet Devoid of Sexual Predators Act of 2008*** – or "**KIDS Act of 2008"** – requires sex offenders to register their email addresses and other Internet identifiers with the National Sex Offender Registry.[188] This information is exempt from public disclosure, but social networking sites are allowed to compare their records against the database.

Senate Bill S.1738 "***Providing Resources, Officers and Technology to Eradicate Cyber Threats to Our Children Act of 2008***" – or "**PROTECT Our Children Act of 2008**" – creates reporting requirements for electronic communications service providers and remote computing service providers who discover content, correspondence and other illegal activities related to child abuse and child pornography.[189] If they have identified an individual who appears to have violated the law, they must provide law enforcement authorities with the identity of the individual, his email address, IP address, URL, and other identifying information that they may have collected.[190] Failure to do so exposes the service provider to a fine of up to $150,000 for an initial violation, and up to $300,000 for subsequent violations.[191]

State Legislation

State legislators have been very active, as well. Numerous bills requiring age verification measures on websites were proposed, such as in North Carolina and Connecticut in 2007, and Georgia[192], Illinois,[193] Iowa[194] and Mississippi[195] in 2008. In

[188] Senate Bill S. 431 has been codified at Public Law N. 110-400.
[189] Senate Bill 1738 has been codified at Public Law N. 110-401.
[190] PROTECT Our Children Act Section 501(a) has been codified as 12 USC 2258A (b).
[191] PROTECT Our Children Act Section 501(a), has been codified as 12 USC 2258A (e).
[192] S. 59.
[193] HB 4874.
[194] HF 2202.
[195] HB 2586; died in Commission.

addition, bills mandating that convicted sex offenders register their email addresses with the state were also introduced by Kentucky, Virginia, and Arizona legislators.

Foreign Activities

Abroad, several countries have issued recommendation and guidance on the protection of children online in connection with access to social networking sites.

United Kingdom

In April 2008, the United Kingdom issued a social networking guidance for the industry, parents and children, aimed at helping teens and tweens interact safely on the Internet.[196] The comprehensive report recommends that social networking websites offer strong privacy protection procedures, and use identity authentication measures. The report provides an extensive list of recommendations.

Spain

More recently, the Spanish Data Protection Agency published a privacy handbook for children and parents with recommendations on using appropriate safeguards while online.[197] The handbook provides a basic overview of the fundamental data protection principles set forth in the Spanish Data Protection Act, addresses the privacy risks to which minors are exposed, and provides recommendations.

New Rules Affecting Social Networking Sites

State Attorneys General have initiated investigations against major social networking sites. In the United States, these investigations culminated with settlements between MySpace and Facebook and a coalition of 49 State Attorneys General. These settlements provide guidelines for social networking sites.

Myspace

In its January 2008 settlement, MySpace agreed to implement design and functionality changes to its site, and to develop education and tools for parents, educators, and children.[198] MySpace will cooperate with law enforcement to deter and prosecute criminals misusing the Internet, and develop a new set of privacy protection standards.

---

[196] http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance.

[197] http://www.ibls.com/internet_law_news_portal_view.aspx?s=sa&id=1426.

[198] See attachment to North Carolina Attorney General Press Release at http://www.ncdoj.com/News-and-Alerts/News-Releases-and-Advisories/Press-Releases/AG-Cooper-announces-landmark-agreement-to-protect-.aspx.

MySpace will hire a third party to compile a registry of email addresses provided by parents who want to restrict their children's access to the website. It will bar anyone using an email address listed in the registry from signing up or creating a user page profile. In addition, MySpace will work to improve the algorithm used to check for underage users.

In order to protect members under 18, MySpace will automatically change the default setting from "public" to "private" for profiles of users under 18, and restrict requests from others to be their "friends". It will keep closed a section of its site called "high school" for users under 18, so that users under 18 can block all users over 18 from viewing their profile or contacting them. In addition, MySpace will organize, with the support of the Attorneys General, an industry-wide Internet Safety Technical Task Force devoted to finding and developing online safety tools and online authentication tools and to establishing specific objective criteria that will be used to evaluate technology safety solutions. AOL, ATT, CDT, Facebook, Google, Linden Lab, Microsoft, MySpace, Verizon, and Yahoo! have joined this taskforce.

Facebook

In May 2008, Facebook entered into a similar settlement when it agreed to add more than 40 safeguards to protect young users from sexual predators and cyber bullies. It will ban convicted sex offenders from the site and will limit older users' ability to search online for subscribers under 18. Facebook will ensure that companies offering services on the site comply with the new safety and privacy guidelines. Like MySpace, Facebook has agreed to build a taskforce seeking ways to better verify users' age and identity.

Other Existing Legal Models

In the United States, laws, regulations, and best practices have been in place for several years to attempt to protect children from the dangers of venturing into the adults' world. One of the most important laws in this area is the **Children's Online Privacy Protection Act ("COPPA")**.[199] COPPA is limited to the protection of minors under 13.

Children's Online Privacy Protection Act

COPPA applies to websites that are directed to children under 13 or have actual knowledge that children under 13 use the site. The law regulates the collection online of information about a child, such as full name, home address, email address, and hobbies. The protected information also includes information collected through cookies and other types of tracking mechanisms when they are tied to individually identifiable information. The law requires websites to identify users who are under 13. When a user

[199] 15 U.S.C. § 6501-6506 (Pub. L. 105-277, enacted October 21, 1998).

is identified as under 13, the interaction with the children and the collection, use, or retention of the child's data must be conducted in a manner consistent with the requirements of the law and its related Children Online Privacy Protection Rule.

The FTC has provided guidance on screening methods. websites must use an age screening mechanism that asks users to provide age in a way that does not invite falsification (neutral age-screening). For example, a drop down menu for users to enter the year of birth would be good. However, a drop down menu that allows users to enter birth years only making them 13 or older would not be considered neutral. A temporary or permanent cookie may be used to prevent users from back buttoning and entering a new age to circumvent the screening mechanisms.[200]

Enforcement of COPPA by the Federal Trade Commission (FTC)

Since the late 1990's, the FTC has conducted numerous enforcement actions against sites whose practices with respect to children's' information were questionable. Its enforcement action against Sony has been one of the most spectacular because of the amount of the fine assessed against the company. The $1 million fine assessed against the company remains the largest fine ever assessed by the FTC against a site in connection with the protection of children's information.

In December 2008, the FTC concluded an enforcement action against Sony BMG Music Entertainment ("Sony") under charges that Sony had violated COPPA and Section 5 of the FTC Act.[201] According to the FTC complaints, in the websites that Sony operated for its artists and labels, users were required to submit a broad range of personal information, including date of birth, in order to register. On 196 of these sites, Sony collected personal information from thousands of underage fans without first obtaining their parents' consent.[202] Many of these sites also enabled children to engage in private messaging, which allowed them to interact with others, including adults.

The FTC alleged that Sony violated COPPA by failing to provide sufficient notice of the type of information the company collects from children, how it uses this information, and what information it shares with others, that Sony failed to provide parents with notices of its information practices, to obtain their verifiable consent, and to provide them with means to review the personal information collected from their children or to refuse to permit further use or maintenance of this information.[203] Additionally, the FTC charged Sony with violating Section 5 of the FTC Act by falsely stating in its

---

[200] Children's Online Privacy Protection Rule, http://www.ftc.gov/privacy/privacyinitiatives/childrens_lr.html.

[201] Complaint, *United States v. Sony BMG Music Entm't*, No. 08 CV 10730 (F.T.C. Dec. 11, 2008), *available at* http://www.ftc.gov/os/caselist/0823071/index.shtm.

[202] http://www.ftc.gov/opa/2008/12/sonymusic.shtm

[203] *Id.*.

privacy policy that users who indicate that they are under 13 will be restricted from participating the Sony activities.[204] Actually, Sony accepted registrations from users who entered a date of birth indicating that they were under 13, and allowed them to use the site.[205]

The December 2008 Consent Decree calls for Sony to pay a $1 million fine, and to delete all personal information collected and maintained in violation of the law since April 21, 2000.[206] The Consent Decree also has a significant education component in addition to numerous reporting and recording keeping requirements.[207] Sony must also educate children who use its sites and their parents, about children's privacy in general, and social networking in particular.[208] For five years from the date of entry of the Consent Decree, the company must place clear and conspicuous notices throughout its sites to invite parents and children to visit the FTC materials related to children's privacy and social networking.[209] There are additional compliance, reporting, and record keeping provisions. For example, for three years from the date of the consent decree, Sony must maintain and make available to the FTC, all documents demonstrating compliance with the Consent Decree.[210] Moreover, each document must be retained for at least two years after its creation.[211]

State Action Under COPPA

In April 2008, the Texas State Attorney General completed an action under COPPA, in the case *Texas v. Doll Palace Corp.* W.D. Tex. (Texas April 2008). In this case, the site required users, as part of the sign-up registration process, to provide their age. The users were then presented with a screen stating "The site requires that you have permission from a parent if you are under 13. Do you have a parent with you now?" Following the statement, the user was required to click a "yes" or "no" box in order to continue. The Texas Attorney General found this practice questionable, and stated:

> "*Companies cannot take on a veil of innocence by hinting to underage users ways to bypass age verification requirements*."

---

[204] *Id.* at 9.

[205] *Id.*

[206] Consent Decree, *United States v. Sony BMG Music Entm't*, No. 08 CV 10730 (F.T.C. Dec. 11, 2008), *available at* http://www.ftc.gov/os/caselist/0823071/index.shtm.

[207] *See generally* http://www.ftc.gov/os/caselist/0823071/081211consentp0823071.pdf

[208] http://www.ftc.gov/os/caselist/0823071/081211consentp0823071.pdf

[209] http://www.ftc.gov/os/caselist/0823071/081211consentp0823071.pdf

[210] *Id.* at 9.

[211] *Id.*

Children's Internet Protection Act

The **Children's Internet Protection Act** or "**CIPA**"[212] requires schools and libraries using the E-Rate Discount[213] to use technology protection measures with respect to any of their computers with Internet access, in order to prevent access to visual depictions that are obscene, child pornography or harmful to minors. These measures must be active when the library computers are used by minors. The library may disable the protection during use by an adult, to enable *bona fide* research and other lawful purposes.[214]

Child Registry Laws

States have taken numerous initiatives, as well. Utah and Michigan attempted to protect minors from solicitations for the purchase of illegal products or substances (such as alcohol) by enacting their Child Registry Laws in 2005. Both of these laws allow individuals to register "contact points" of minors (<18). These contact points include email address, phone number, and fax number. The laws prohibit sending a communication to a contact point that is registered in the State Registry if the communication advertises a product or service that a minor is prohibited by law from purchasing, or that is harmful to minors: gambling, pornography, alcohol, tobacco, and illegal and prescription drugs.[215] The Registries that maintain the lists of "contact points" are kept under the authority of the State of Utah and State of Michigan. Marketers who wish to advertise products or services that are covered by the law must compare their list against the registry list before sending their emails.

Electronic Authentication

To date, legislators have stayed away from requiring age verification, and have opted to address the issue of child predators and dangers of social networking through measures that would prevent sex offenders from accessing the sites. However, the need for authentication of users and verification of their age and identity remain, in particular when trying to shield children and minors from child predators and other individuals who can cause irreversible harm to minors. Many powerful ways are available, such as

---

[212] Pub. L. No. 106-554

[213] The E-Rate discount is a discount granted to libraries and schools when they purchase Internet access and computers.

[214] The constitutionality of the Children's Internet Protection Act was challenged on First Amendment grounds in the case American Library Association v. United States filed in Pennsylvania. After appeals, the case was reviewed by the U.S. Supreme Court in 2003. The Court held that the use of filtering software by libraries does not violate their patrons' First Amendment right, and that CIPA does not induce libraries to violate the Constitution.

[215] Interestingly, the legal drinking age in the United States is 21. The Child Registry Laws would not shield individuals between 18 and 21 from offers to purchase alcohol even though it is illegal for them to purchase alcohol.

electronic authentication. Age verification mechanisms are currently available in commerce.[216]

Using a technical method for age verification, however, poses serious technical and legal problems.[217] In order to verify the age of a person, an organization is likely to need access to additional information about the identity of the person. Then, once a person's identity is determined, proper tools must be in place to authenticate the person when the individual returns to the site. These two phases are known as "identification" and "authentication process."[218]

Identity verification through electronic authentication poses numerous legal questions that are beyond the scope of this article. The identification process requires the collection of personal information by the identity provider, and the disclosure of this information to the social networking site (relying party). What information would have to be collected by the identity provider? How much of this information may it disclose to the relying party? What security measures should be used to protect the information? Can this information be reused for purposes other than identification, such as targeted marketing? If information is transferred across borders, foreign laws restricting the transfer of information outside a country may apply. How to address the discrepancies between different laws? There are also liability concerns. What happens if there is a faulty authentication and the applicant is granted access to the site or to the system when he should have been excluded? Who will bear the risk associated with a faulty authentication?

Other Complex Issues

There are many issues surrounding the concept of age verification.[219] Verifying a person's age in cyberspace is likely to require access to more information than just age so that the person is authenticated. When the disclosure of a person's identity is required, numerous privacy and security concerns arise. There are also concerns about errors, the consequences for these errors (data spills, people being wrongfully accused, identity theft) and the liability for these errors. There are also questions about human rights.

---

[216] See, e.g. IDology Inc, at, http://www.idology.com/.

[217] See, e.g., OECD Recommendation on Electronic Authentication, and OECD Guidance for Electronic Authentication, http://www.oecd.org/dataoecd/32/45/38921342.pdf.

[218] Thomas J. Smedinghoff and David A. Wheeler, Addressing the Legal Challenge of Federate Identity Management, BNA Privacy & Security Law Report (March 3, 2008)

[219] See, e.g., MySpace Coming of Age for Coming of Age, Leslie Harris, Center for Democracy and Technology; http://abcnews.go.com/Technology/story?id=4355851&page=1.

Data Security and Data Control

New laws are requiring website owners to scrub their databases against public databases in order to identify which users must be removed or denied entry. In order to be able to verify that an individual is not part of an excluded category, databases will have to be created. Who would be responsible for managing these databases? Which security measures would have to be used to protect this information? How would errors be identified and corrected?

How to Ensure Adequate Authentication and Identification

In order to be effective and efficient, age verification systems require the collection of personal information. As such, it is privacy invasive. In order to protect children, should all adults only be "tagged," so that an individual who is not "tagged" would be deemed a child if he or she is not listed on the age verification databases? What would be the content of such a database, and how much information would be required to authenticate a person and label that person an "adult"? How about the marginal cases, such as individuals who are no longer minors but are intellectually challenged or legally incompetent?

Duration of the Authorization

While age verification may work at the time of the initial registration, how about the other uses of the site? Once a user has been authenticated and has received a user name and password, how does a website operator know with some certainty that the individual who logs in on the website with that username and password is the same as the one who initially signed on and provided personal details? In many households, the entire family shares one computer. Different users might not have different accounts.

Privacy and Anonymity

Even if all websites were classified or labeled "PG 13" or "R", as are movies or video games , and if it were possible to create a technical solution that would be easy to implement, it would still be necessary to balance the legitimate individual rights and freedoms against the need to protect children from predators or from content that might not be suited to them. Identification requires knowledge of, and access to personal data. Would it be possible to have robust age verification, but still protect privacy? Would the right to access information anonymously be undermined?

Constitutional Law or Human Rights Issues

The constitutions of many countries provide the citizens and residents of these countries with extensive rights. Would excluding minors from social networking sites,

virtual worlds, multiplayer gaming sites, and the like violate the children's constitutional rights to free speech (in the US) or similar rights? Would age verification aimed at minors, but necessarily required of all users, pass constitutional scrutiny if it burdens the free expression of adults?

In the United States, the Communication Decency Act of 1996,[220] which attempted to regulate pornographic material (when available to children) on the Internet has been partially overturned. The indecency provisions were held to be an unconstitutional abridgement of the First Amendment Right to Free Speech because they did not permit parents to decide for themselves what material was acceptable for their children.

Similarly, the "Children Online Protection Act" or "COPA" (not to be confused with the Children Online Privacy Protection Act or COPPA),[221] which was adopted to restrict access to material defined as harmful to minors on the Internet, has been repeatedly struck down by courts on the grounds that it violates the constitutional right to free speech under the First Amendment to the Constitution of the United States.[222]

Global Issues

There are more issues, which stem from the global reach of the Internet. If age verification technologies were efficient, cost effective, and available, would they achieve the goal of protecting children from adult content, and would they shield children from predators? Given that the Internet can be accessed from anywhere in the world, would barriers created in one country prove to be useless or inefficient in a global economy?

A country-centric age verification regime would fail when minors can access foreign-based websites located in more permissive legal regimes. Furthermore, even if countries wanted to cooperate on age verification, they would be hampered by thorny definition issues. How would "minor" be defined? There is no consensus globally. While most countries have adopted 18 as the age of majority, in Japan, Taiwan, Thailand, and the Republic of Korea, the age of majority is 20. In Singapore, Monaco, Honduras, or Egypt, it is 21. The same disparities appear in the United States. While the age of majority is 18 in most US States, it is 19 in Alabama and Nebraska, and 21 in the District of Columbia and Mississippi.[223] With such disparities, the implementation of a global age verification regime becomes highly problematic.

Conclusion

---

[220] 47 U.S.C. § 223.

[221] 47 U.S.C. § 231.

[222] See also the (unsuccessful) challenges to the Children's Internet Protection Act, above, on grounds of First Amendment violation.

[223] Wikipedia: http://en.wikipedia.org/wiki/Age_of_majority.

Is age verification the cure to the problem of child predators? Will it help shield children from access to controlled substances or questionable materials? Can we hope to succeed in identifying and authenticating individuals on the Internet when children's creativity and ingenuity – and adults' complacency – have made it impossible to achieve reliable identification or authentication in the brick and mortar world?

In the brick and mortar world, where it is arguably easier to compare a live person to the photo attached to an identification document, society is struggling to prevent teens from using fake identification documents and other fraudulent means to purchase alcohol and tobacco, or access restricted content. When children use fake identification documents, the clerk at the liquor store does not verify the actual identity of the person; he only verifies the content of the documents the person provides. How can we expect to succeed in cyberspace where there is even less ability to conduct a reliable identity check than in the brick and mortar world? Does it make sense to replicate a model that has shown so many flaws?

Until a better solution can be found, parents and schools remain the most logical place to turn. They have an important role to play. Educating children about the dangers that they might encounter on the Internet, and teaching children the appropriate ways to use the Internet would definitely contribute to the better safety of these sites.

NET NEUTRALITY

NET NEUTRALITY

Bennet Kelley

With advocates gathering over one million signatures to petition Congress and supporters including Internet godfather Vint Cerf, television and recording artists such as Alyssa Milano, the Dixie Chicks and Moby, liberal groups such as MoveOn.org and the ACLU as well as conservative groups as the Christian Coalition and Gun Owners of America, Net Neutrality was the hot tech issue in 2006. To Net Neutrality critics, such as Federal Communications Commission ("FCC") Commissioner Deborah Taylor Tate and AT&T Chief Executive Officer Edward Whiteacre, the movement is based on a term that has no meaning.[224]

The issue was triggered by the 2005 Supreme Court's decision in *National Cable & Telecommunications Association et al. v. Brand X Internet Services* and subsequent FCC decision that broadband Internet service was not a "telecommunication service" subject to mandatory regulation as a common carrier under Title II of the Federal Communications Act, but was an "information service" subject to the less stringent requirements of Title I.[225] As a result, instead of mandatory nondiscrimination rules, broadband providers are subject to the following nonbinding FCC guidelines:

- To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to access the lawful Internet content of their choice.
- To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.
- To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do not harm the network.
- To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to Competition among network providers, application and service providers, and content providers.[226]

---

[224] R. Michael Senkowski and Shawn A. Bone, Net Neutrality Primer 3 (June 2006) http://www.wileyrein.com/docs/publications/12598.pdf.

[225] *National Cable & Telecommunications Association* v. *Brand X Internet Services*, 545 U.S. 967 (2005), Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 02-33 (September 23, 2005) ("FCC Guidelines").

[226] FCC Guidelines, *supra* note 6, at 3.

Concerns that the cable and telecommunications companies would seek to become gatekeepers of the Internet were ignited by AT&T's Whiteacre's comment that Internet companies

> would like . . . to use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. . . . The Internet can't be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo or Vonage or anybody to expect to use these pipes free is nuts.[227]

Net Neutrality proponents argued that legislation was required to stop Whiteacre and others from dictating the content and technologies available to Internet users. Opponents, however, contend that the Internet has flourished because it has been unregulated and that burdensome regulations and resulting litigation would reduce the incentive for broadband providers to invest in additional infrastructure.[228]

Net Neutrality failed in the last Congress as advocates simply were outmanned by the cable and telecommunications lobby, but they did score a minor victory when the AT&T/Bell South merger was held up by a deadlocked FCC until AT&T committed "that it will maintain a neutral network and neutral routing in its wireline broadband Internet access service." In approving the merger, however, FCC Chairman Martin and Commissioner Tate released a statement that the conditions imposed on AT&T were "discriminatory and run contrary to commission policy and precedent" and does not mean that the FCC has embraced Net Neutrality.[229]

By 2008, despite the fact that some of the very dangers that they warned of have occurred or may soon occur, the movement seemed to have less traction than before.[230] It would surely be a tragic irony that a medium that has done so much to revolutionize political campaigns through increased mobilization was somehow incapable of mobilizing to defend itself. Neutrality proponents scored a minor success when House Judiciary Committee Chairman John Conyers offered the "Internet Freedom and

---

[227] Arsad Mohammed, *SBC Head Ignites Access Debate*, Washington Post, November 4, 2005 at D-1 http://www.washingtonpost.com/wp-dyn/content/article/2005/11/03/AR2005110302211.html.

[228] Angele A. Gilroy, *Net Neutrality: Background and Issues* (Congressional Research Service (May 16, 2006) at 4-5 http://www.fas.org/sgp/crs/misc/RS22444.pdf..

[229] Rhonda Ascierto, *FCC Chair Rallies against Net Neutrality for All*, Computer Business Review Online (February 2, 2007) http://www.cbronline.com/article_news.asp?guid=017C23F1-1A86-4516-B88B-4929A3AEB467.

[230] See, e.g., Peter Svensson, *AT&T Weighs Extra Fee for Heavy Bandwidth Use*, Free Press, June 13, 2008, http://www.freepress.net/node/41568.

Nondiscrimination Act of 2008", which would treat any discrimination in Internet access as an antitrust violation.[231]

As in 2007, the key events for net neutrality in 2008 centered on Chairman Martin and the FCC.

The FCC returned to the debate after Comcast interfered with access to BitTorrent and other P2P applications as part of its "network management" efforts without disclosing this to its subscribers. Chairman Martin, however, was now a convert to Net Neutrality and relied on the FCC Guidelines to find that Comcast's

> discriminatory and arbitrary practice unduly squelches the dynamic benefits of an open and accessible Internet and does not constitute reasonable network management." Moreover, Comcast's failure to disclose the company's practice to its customers has compounded the harm.[232]

Comcast has appealed the FCC's Order.

---

[231] H.R. 5994, 110th Congress, http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.5994:; *Conyers and Lofgren Introduce Net Neutrality Legislation to Protect the Internet from Anticompetitive Practices*, *Free Press,* May 8, 2008, http://www.freepress.net/node/39684. The Conyers bill competes with House Telecommunications and the Internet Subcommittee Chairman Ed Markey's Internet Freedom Preservation Act of 2008. H.R. 5353, 110th Congress, *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h5353ih.txt.pdf*.

[232] Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, File No. EB-08-IH-1518, Memorandum Opinion and Order, FCC 08-183 (rel. Aug. 20, 2008); available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.doc. See also Notice of *Ex Parte* Presentation Free Press, *et al*., Petition for Declaratory Ruling CC Docket No. 02-33, CC Docket No. 01-337, CC Docket Nos. 95-20; "Can the F.C.C. Enforce 'Network Neutrality?'" *Conde Nast Portfolio*, Apr. 22 2008, http://www.portfolio.com/views/blogs/daily-brief/2008/04/22/can-the-fcc-enforce-network-neutrality; "Comcast Says FCC Has No Authority to Stop Traffic Shaping," TechDirt, Mar. 20, 2008, http://ww.techdirt.com/articles/20080319/195617592.shtml.

GLOSSARY OF TERMS

GLOSSARY

ACPA (also known as Anti-Cybersquatting Consumer Protection Act) - A federal law (codified at 15 U.S.C. § 1125(d)) enacted in 1999 to allow for civil penalties when the defendant has registered a domain name which is either a trademarked term, or an individual's name, for the sole purpose of earning a profit by selling the domain to the trademark holder or individual.

Active Tag (in RFID) - A type of RFID tag (see definition below) that is equipped with a battery.

Age Verification - A variety of methods used by websites to confirm the age of the website user.

Anti-Cybersquatting Consumer Protection Act (also known as ACPA) - See ACPA, above.

Behavioral Targeting - A collection of methods by which an online advertiser can track a user's behavior and then customize the user's experience to increase the probability the user will purchase products or services from the seller.

California Online Privacy Protection Act of 2003 - A state law (codified at California Business & Professions Code §§ 22575-22579) that requires online operators of websites that collect personally identifiable information to post information about their privacy policies.

CAN-SPAM Act (as known as the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) - Federal anti-spam legislation that was passed at the end of 2002, and became effective on January 1, 2003. The CAN-SPAM act has many sections devoted to defining and outlining what are acceptable practices for the sending of commercial email, and criminalizes the worst practices.

ccTLD (also known as Country-code Top Level Domain) - One of a number of top level domain names typically reserved for use by residents, entities, or agencies of a particular country, e.g., the ".us" part of the domain name in "http://ci.sacramento.ca.us", the website for the City of Sacramento.

CDA (also known as Communications Decency Act) - A federal anti-pornography law which is aimed at regulating pornography on several media venues, including television, radio, and the Internet. Among other things, the CDA criminalizes knowingly using the Internet to transmit, send, or display, to a person under the age of 18, "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."

Children's Online Privacy Protection Act (also known as COPPA) – A federal law enacted in 1998 that governs the collection of information at websites that are geared

towards children under the age of thirteen, or websites where the website operator has or should have knowledge that children under the age of thirteen frequent the website. COPPA also governs the disclosure of that information, particularly with regards to parental requests for information to protect online privacy of children under the age of thirteen.

Children's Internet Protection Act (also known as CIPA) - Federal law that requires that any school or library which has received benefits through the Federal E-Rate program must have in place on all Internet-connected computers measures to protect users of those computers from "visual depictions that are obscene, child pornography, or harmful to minors."

CIPA - See Children's Internet Protection Act above.

Cloud computing - Cloud computing involves virtual resources which are provided as a service over the Internet, "cloud" being a metaphor for the Internet and its complex infrastructure. A user does not need to have knowledge of or control over the technology infrastructure in the "cloud" that supports him or her. The concept of cloud computing encompasses software as a service (SaaS) and common business applications that are online and may be accessed from a web browser. See also **SaaS.**

Communications Decency Act (also known as CDA) – See above.

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (also known as the CAN-SPAM Act) – See above.

Cookie – A "cookie" is a small text file that is created and placed on one's computer when one visits certain websites.

COPPA (also known as Children's Online Privacy Protection Act) – See above.

Country-code Top Level Domain (also known as ccTLD) – See above.

Cyberbullying – The act of cyberstalking someone with the intent to scare, harm, embarrass, or intimidate the victim, where the victim is a minor.

Cybersquatting – The practice of obtaining a domain name that consists of or contains the trademark of another person or entity, for the purpose of trying to sell it to that person or entity for a price.

Cyberstalking - The act of watching, pursuing, and/or harassing someone using online (on the Internet) means and methods. It can include, but is not limited to, repeatedly sending unwanted or unwelcome email, instant messages, text messages or other Internet-based messages to the victim after being asked to desist, sending such messages to a third-party where the victim is the subject of the message, or posting such messages about or directed to the victim in public or private forums or social networking sites.

Cyberspace – The entire "world" of the Internet and all of its content, including but not limited to the World Wide Web, electronic mail, and all other "places" one can see or go on the Internet.

Data - A general term applied to any piece of information which can reside on a computer. This includes, but is not limited to, user information, files, graphics, computer programs, and the code of which computer programs are constructed.

Data Security – The practice of keeping electronic data secure from unwanted access or corruption.

Dodos - Dodos stands for "Distributed Denial of Service." It is sometimes abbreviated to just "DoS" (Denial of Service). A DoS attack is one in which many Internet-connected computers under the control of a malfeasor are used to flood the target computer system with data such as to overwhelm the target system, jamming the target system's bandwidth and effectively or actually taking the target system offline.

Digital Millennium Copyright Act (also known as the DMCA) – A federal law enacted in 1998 that addresses many aspects of Internet piracy and copyright infringement, the highlights of which include criminalizing the circumvention of anti-piracy measures built into software and the manufacture of such circumventing devices and software; creating a relatively simple mechanism for copyright holders to demand that infringing material be taken down from public Internet sites (see "DMCA Takedown Notice"); and providing a "safe harbor" for internet service providers (ISPs) when such infringing material has been published by their users without the Internet Service Provider's knowledge. See also **ISP**.

DMCA (also known as the Digital Millennium Copyright Act) – See above.

DMCA Takedown Notice: A DMCA Takedown Notice is a notice sent, pursuant to the DMCA, to an Internet provider or other Internet site, demanding that material which appears on the site, and which infringes on the noticer's copyright, be removed ("taken down") from the site. See also **DMCA**.

DNS: DNS stands for the "Domain Name System," and is the infrastructure that correlates a domain name (such as "isipp.com") with the IP address number actually assigned to the computer at which the domain is hosted. For example, the domain "isipp.com" is hosted on a computer at the IP address 69.12.213.226. The IP address 69.12.213.226 is meaningful to other computers attempting to contact the isipp.com site, but to a human end user, the domain "isipp.com" is more meaningful than is "69.12.213.226." The Domain Name System translates between the two (domains and IP addresses). See also **IP Address** and **Domain Name**.

Domain or Domain Name: A domain name is a registered identifier which, when the registering party associates it with a particular computer server which is connected to a particular IP address in the Internet, identifies a location on the Internet to which email, web browsers, and other Internet communications protocols can be directed. For example, the domain ISIPP.com is registered to the organization known as ISIPP.

Without being associated with ISIPP's computer server, the location of which on the Internet is determined by the IP address to which the server is connected, the domain ISIPP.com is virtually meaningless. However, once associated by DNS records with the IP address on the Internet assigned to ISIPP, to which ISIPP's computer server is connected, the domain ISIPP.com becomes an address on the Internet to which email can be sent, and web browsers can be directed. See also **DNS**.

Domain Name Registrar – One of a number of services that is responsible for establishing and maintaining the unique domain name for a computer or service that is connected to the Internet.

Domain Name System (also known as **DNS**) – See above.

ECPA (also known as Electronic Communications Privacy Act) – A federal law enacted in 1986 (codified in various sections of Title 18 of the United States Code) that criminalized certain unauthorized accesses and uses of electronic communications and stored data.

Electronic Communications Privacy Act (also known as ECPA) – See above.

EU Privacy "Safe Harbor" Guidelines – Privacy policy guidelines established by the European Union that, if followed, provide a "safe harbor" from liability for the use or disclosure of personally identifiable information.

EU Privacy Directive – A directive adopted by the European Union Council of Ministers in 1995 to provide guidelines for the collection, protection, disclosure, and use of private information by website owners and operators.

Generic Top Level Domain (also known as gTLD) – The most common of the three categories of top level domains recognized by the Internet Assigned Numbers Authority, including .com, .net, and .org.

Global Positioning System (also known as GPS) – A global navigation system that uses signals from four or more orbiting satellites to determine precise latitude, longitude, elevation, and time.

GPS (also known as Global Positioning System) – See above.

Gramm-Leach Bliley Act – Also known as the Financial Services Modernization Act of 1999, this Act repealed the Glass-Steagall Act of 1933 and allowed for consolidation of commercial banks, investment banks, securities firms, and insurance companies.

Gripe Site – A website devoted to criticism or mockery of somebody or something.

gTLD (also known as Generic Top Level Domain) – See above.

Hacking – A broad term referring to reprogramming or reconfiguring a computer system to function in ways not intended by the developer or owner of the system.

Health Insurance Portability and Accountability Act of 1996 (also known as HIPAA) – A federal law enacted in 1996 to regulate health insurance plans and to provide certain protections relating to the use and disclosure of health-related information.

HIPAA (also known as Health Insurance Portability and Accountability Act of 1996) – See above.

ICANN (also known as Internet Corporation for Assigned Names and Numbers) – A nonprofit corporation originally created in 1998 by act of the United States government to assume responsibility for the assignment and management of domain names and other Internet-related responsibilities.

Identity Theft – The practice of taking personally identifiable information of another person, such as credit card or social security numbers, without authorization, for purposes of theft, fraud, or personal gain.

Initial Interest Confusion - A form of consumer confusion that exists when a person visits a website or other Internet location because of its use of another's trademark in its web advertising or search strategies.

Internet Child Registry: An Internet child registry is a repository of email addresses which belong to or are accessed by minors. Currently two states, Michigan and Utah, maintain Internet Child Registries, and commercial email senders who may send email with content that is not suitable for minors are required to "scrub" their mailing lists against the registries in order to have all registered email addresses removed from their mailing lists. Registration with the Internet Child Registries is on a voluntary basis, and the usefulness and validity of the Internet Child Registries is a source of some disagreement.

Internet Search Engine: An Internet Search Engine is any program or service which operates on the Internet and which is designed to allow the user to perform a search across the Internet or part of the Internet, usually based on keywords or phrases.

IP Address: IP Address is short for "Internet Protocol Address." An IP address is analogous to a telephone number. It is the numeric way of addressing a computer connection to the Internet, in the same way that a telephone number is a telephone connection to the telephone system. Given a known telephone number, one can hook up any sort of telephone to the telephone connection, and it will still have the same telephone number. Similarly, given a known IP address associated with an Internet connection, one can hook up any computer to that connection, and it will still have the same IP address. The one exception to this is that some Internet services provide what is known as "dynamic IP addressing", meaning that every time an Internet connection is opened, the connection is assigned a different IP address, rather than it always having the same IP address. IP addresses are obtained from one's Internet Service Provider (ISP). See also **ISP**.

Internet Corporation for Assigned Names and Numbers (also known as ICANN) – See above.

Internet Service Provider (also known as ISP) – A company that contracts with a customer to provide the customer access to the Internet.

ISP (also known as Internet Service Provider) – See above.

Keylogging – Also "keystroke logging," the practice of covertly tracking the keys struck by a computer user on the user's computer keyboard.

Keyword - A keyword in the context of the Internet most often refers to specific terms which are associated with the subject matter and content of a particular page or site on the Internet. Search engines such as Google return search results based on the keywords upon which someone searches. Refining the terms (keywords) one uses in articles published on the Internet so as to optimize the number of searches that will result in your site being listed in the search engine results is considered something of an art, and is one of the functions of Search Engine Optimization (SEO). See also **SEO** and **Internet Search Engine**.

Malware: Malware is short for "malicious software," and is the general term used to describe any malicious code or software which accesses and deploys itself on a user's computer without the user's knowledge or consent. The term "malware" includes computer worms, computer trojans, computer viruses, and spyware. See also **Spyware**.

MMORPG: MMORPG stands for a "Massively Multiplayer Online Role-Playing Game." A MMORPG is one in which many players can access the game - usually an online virtual world - across the Internet. The most well-known MMORPG is World of Warcraft.

Net Neutrality – A principle for open access by users to the internet regardless of content, sites, equipment or platforms. This includes access to content such as digital video that requires a large amount of bandwidth (capacity) over broadband networks.

Online Profiling - Methods and practices by which website owners gather and use information about the visitors to websites, specifically by constructing and using a profile of the visitors by analysis of behavioral data arising from the websites (clicking on links, past purchase history and the like) and demographic data.

P2P (also known as Peer-to-Peer) – An approach that uses a decentralized network configuration to enable resources (such as computer processing power, data storage or network bandwidth) controlled by participants to be shared directly with other participants, without central coordination or control. Although P2P provides the ability to share resources at low cost and high speed, it has been controversial as an enabling technology for the unauthorized sharing of copyrighted works.

Passive Tag (in RFID) – A type of RFID tag are that has no internal power source and performs no actions until it is awakened by the radio signal emitted by a reader device.

Peer-to-Peer (also known as P2P) – see P2P.

Personally Identifiable Information (also known as PII) - Information that can be used to identify a specific individual person. PII is defined and legally protected under

numerous federal and state privacy laws, including but not limited to California's security breach disclosure laws (Civil Code §§ 1798.29-1798.82 and 1798.84).

Phishing – Obtaining user information (such as user names, passwords, social security numbers and credit card numbers) through fraud. Phishing facilitates identity theft. This is often done via an email which has an official appearance (and a forged return address), but which directs the user to a fake website where the user's information is collected.

Pretexting - The impersonation of a customer or authority figure (such as a police or tax investigator) in order to obtain information. It includes the sale or use of telephone records obtained by persons pretending to be actual telephone company subscribers.

Privacy Policy – A written policy that describes how a website owner will collect and use information gathered from visitors to the website.

Protest Website – A website that protests an individual or organization and that uses the name or trademarks of the individual or organization in its domain name. Such uses of a domain name raise questions of fair use under trademark law.

Radio Frequency Identification Device (also known as RFID) - A generic term for technologies that use radio waves to automatically identify people or objects from a distance of several inches to hundreds of feet.

Reverse Domain Name Hijacking – A domain name dispute initiated with the goal of taking a domain name away from a registrant who is equally entitled to use it.

RFID (also known as Radio Frequency Identification Device) – See Radio Frequency Identification Device.

SaaS - SaaS (pronounced "sass") stands for "Software as a Service." It is a model of software delivery in which a provider licenses an application to customers to use as a service on demand. SaaS software vendors may host the application on their own web servers or download the application to a consumer device, disabling it after use or after the on-demand contract expires. In any event, the vendor provides daily technical operation, maintenance, and support for the client. See also **Cloud Computing**.

Short Message Service (also known as SMS, Texting, or Text Messaging) – See Text Messaging. Although Short Message Service and SMS are specifically a text transmission protocol, the terms are used colloquially to include cell phone data messaging that includes images, video and sound.

Sexting - Sexting is the act of sending nude or partially nude pictures of oneself from one's cellphone to another cellphone. The term is almost always applied to underage teens - usually girls. Sexting is illegal in most states, and some teen girls have been prosecuted as sex offenders, and have been required to register on a Sex Offenders Registry upon being convicted of sexting.

Smart Tag (in RFID) – An RFID tag that possesses the technological capability to include some forms of security protection for transmission of sensitive data.

SMS (also known as Short Message Service, Texting, or Text Messaging) – See Short Message Service.

Social Networking – A service offered predominantly through the Internet that permits people to connect with friends and colleagues and form relationships with new individuals. Users typically create an online profile, establish online connections to friends and colleagues, and communicate online through the service by means of email, instant messaging, "news feeds" of recent activities and other means. As of February 2010, prominent social networking services based in California include Facebook, LinkedIn, MySpace, and Twitter.

Spam – In policy discussions, unsolicited commercial email (usually in bulk form). However, as pointed out elsewhere in this Guide, a study by the Pew Internet & American Life Project found that consumers consider spam to be any email they do not want (regardless of whether it is solicited).

Spyware - Software that is downloaded onto a user's computer without their knowledge. It may collect information about a user's activities and transmit that information to someone else. It may change computer settings, or cause "pop-up" advertisements to appear (in that context, it is called "adware"). Spyware may redirect a Web browser to a site different from what the user intended to visit, change the user's home page, or even log keystrokes for malicious purposes.

Text Messaging (also known as Texting, SMS, Short Message Service, or Text Messaging) - A widely used method of sending and receiving brief written messages between mobile phones over cellular telephone networks.

Texting (also known as Text Messaging, SMS, Short Message Service, or Text Messaging) – See Text Messaging.

TLD (also known as Top Level Domain) – See Top Level Domain.

Top Level Domain (also known as TLD) – The label to the right of the last dot of a full domain name. An example is ".com" in "newco.com").

UDRP (also known as Uniform Domain Name Dispute Resolution Policy) – See Uniform Domain Name Dispute Resolution Policy.

Uniform Domain Name Dispute Resolution Policy (also known as UDRP) – A policy that is incorporated into most domain registration agreements, which requires a domain name registrant to submit to arbitration of trademark-related challenges to the domain.

Unsolicited Commercial Email (also known as UCE) – A narrower term than Spam, used for regulatory purposes. UCE would not include, for example, hoaxes and non-commercial chain letters.

URL: The term URL refers to the Uniform Resource Locator, which in common parlance refers to the plain English Internet address of a website (such as http://www.ISIPP.com/). See also **Domain.**

Website – A collection of text, graphics, audio, and/or video content, which is typically formatted in hypertext markup language (HTML), located by means of a Uniform Resource Locator (URL, or domain name), and transmitted to the user over the internet via Hypertext Transport Protocol (HTTP). More familiarly known as a collection of such content that can be viewed by means of web browser software.

Wi-Fi – A trademark of the Wi-Fi Alliance (www.wi-fi.org) for use with certified wireless local area network devices based on IEEE 802.11 standards. Colloquially, a technology used to access the internet wirelessly over a broadband connection.

ABOUT THE CYBERSPACE LAW COMMITTEE

THE CYBERSPACE LAW COMMITTEE

The Cyberspace Law Committee is a Standing Committee of the Business Law Section of the State Bar of California. It consists of 18 attorneys, who are drawn from academia, industry, and the practicing bar. They are appointed by the Business Law Section Executive Committee of the State Bar to three year terms though an application process. In addition, a number of advisors and former members assist the Committee's work. Generally, the Committee promulgates publications and programs primarily aimed at its "constituency," some 1,000 or so State Bar members who have indicated their interest in its work.

The Cyberspace Law Committee's mission includes the following tasks:

- To identify cyberspace law issues that impact businesses and commercial transactions in California.
- To make recommendations on relevant legislation;
- To develop programs, studies and reports on how cyberspace law affects the practice of business law; and
- To develop a website for the collection and dissemination of current developments in cyberspace law.

The Committee holds monthly meetings by teleconference or in person that are open to any interested person. Information about the Committee and contact information for its officers is available on the State Bar website at

http://www.calbar.ca.gov/state/calbar/calbar_generic.jsp?cid=11378&id=7470

ACKNOWLEDGEMENTS

Harry Boadwee is a principal at the Boadwee Law Office in Cupertino. He is a business and corporate lawyer who focuses on technology transactions, software and internet law. He has represented U.S. and international companies and entrepreneurs in matters such as: negotiation of strategic alliances and intellectual property licenses; legal advice about offerings of new technology products and services, particularly software and web services, including free and open source software; and formation and financing of startup companies. Before founding his firm, Mr. Boadwee was Assistant General Counsel of Intuit Inc., makers of Quicken® personal finance software and QuickBooks® small business accounting software. Prior to Intuit, Mr. Boadwee was associated with Fenwick & West LLP (Mountain View, California) and Debevoise & Plimpton LLP (New York, New York). He is the author of *Product Market Definition for Video Programming*, 86 Columbia Law Review 1210 (1986). He also serves on the Cyberspace Law Committee of the Business Law Section of the California State Bar. Mr. Boadwee received his J.D. degree from Columbia Law School, where he was a James Kent Scholar, a Harlan Fiske Stone Scholar, and an Articles Editor of the Columbia Law Review. He received an A.B. in English with distinction from Stanford University, and is a member of Phi Beta Kappa. He also attended the Massachusetts Institute of Technology as an undergraduate, where he was a research assistant at the MIT Architecture Machine Group, the predecessor of the MIT Media Lab.

Stephen L. Davis, of Davis & Leonard, Sacramento, practices transactional counseling and litigation in the areas of copyright, trademarks, trade secrets, unfair competition, the Internet and e-commerce, and art law, as well as general business counseling and litigation. Mr. Davis has extensive experience in civil litigation in state and federal courts, and has prosecuted misdemeanor and felony criminal cases as a deputy district attorney with the Sacramento County District Attorney's Office. He has been an active lecturer on a variety of topics including intellectual property law, the Internet, and art law, and he taught trademark law as an Adjunct Professor at McGeorge School of Law during the 2008-2009 school year. Steve is a former president of the Intellectual Property Law Section of the Sacramento County Bar Association, and serves on the Cyberspace Law Committee of the California State Bar Business Law Section. He also is a member of California Lawyers for the Arts and its attorney referral and mediator panel. Mr. Davis received his A.B., *magna cum laude*, from Harvard University, and his J.D. from the UCLA School of Law, where he was the Chief Managing Editor of the UCLA Law Review and received the American Jurisprudence Award for Federal Courts.

Robert V. Hale II most recently served as Vice President and Senior Counsel at HSBC North America, where he handled consumer, transactional, and litigation matters. Before joining HSBC, Mr. Hale served as Counsel for Golden West Financial (now Wells Fargo), following 8 years at Providian Financial Corporation (now Chase). He is the author of "Wi-Fi Access and Operation Liability," published in The SciTech Lawyer and of the chapter on "Identity Theft" in Privacy Compliance and Litigation (Cal CEB 2008).

Mr. Hale serves on the California State Bar Business Law Section's Financial Institutions Committee and as an incoming Co-Vice Chair of the Business Law Section's Cyberspace Law Committee. He is Executive Managing Editor of the Journal of Internet Law (Aspen Publishers). Mr. Hale received his B.A. from Sarah Lawrence College and his J.D. from the University of San Francisco School of Law.

Francoise Gilbert is the Managing Director of the IT Law Group, a law firm headquartered in Palo Alto, California. Her practice focuses on compliance with privacy, security, and data protection laws and regulations in the United States and abroad. She advises clients on weaving privacy and security into their contracts and all aspects of their business, and developing and implementing data governance strategies and compliance programs. She is the author of *Global Privacy & Security Law* (Aspen Publishers - Wolters Kluwer 2009). Ms. Gilbert is an adjunct faculty member at the University of Illinois in Chicago and a co-chair of the KnowledgeNet (Silicon Valley) of the International Association of Privacy Professionals. She is a founding member and contributor to the Cloud Security Alliance and its General Counsel (probono). Ms. Gilbert has been recognized by *Chambers USA* as a leading lawyer in the field of information privacy and security, and has been selected by her peers for inclusion in the *Best Lawyers in America* and *Who's Who in ecommerce* in the field of information privacy and security. Ms. Gilbert holds undergraduate and graduate degrees in Mathematics and Education from the Universities of Paris and Montpellier (France) and J.D. degrees from both the University of Paris (France) and Loyola University School of Law in Chicago. She is also a Certified Information Privacy Professional (CIPP).

Robert V. Hawn is a partner in Structure Law Group, LLP, in San Jose. His practice emphasizes technology start-up companies, with a special emphasis of technology, transfer, development, and distribution transactions. He speaks and writes frequently on these areas of law and is Co-Vice Chair of the Cyberspace Law Committee of the Business Law Section of the State Bar of California.

Bennet Kelley, an award-winning columnist, blogger, and political analyst, is also a leading Internet attorney and founder of the Internet Law Center. He has been active in many of the hottest Internet issues over the past decade including behavioral targeting, cyber abuse, cybersquatting, Internet marketing, net neutrality, online promotions, online gambling, privacy, spam, and spyware. Prior to founding the Internet Law Center, he was Assistant General Counsel with ValueClick, which he came to through its acquisition of Hi-Speed Media, for whom he was Vice President of Legal & Strategic Affairs. He also served as General Counsel of ETM Entertainment Network. Mr. Kelley is Co-Chair of the Cyberspace Law Committee.

Jean Magistrale is a Publications Attorney in the Business Law Practice Group at California Continuing Education of the Bar (CEB) in Oakland, where she manages, edits, and develops business law publications. She is a Certified Information Privacy

Professional (CIPP); in addition, she serves as a Co-Vice Chair of the Cyberspace Law Committee of the State Bar Business Law Section. Ms. Magistrale received her B.A. from the University of California, Berkeley, and her J.D. from the University of San Francisco School of Law.

Anne P. Mitchell, Esq. is the CEO and President of the Institute for Social Internet Public Policy. Ms. Mitchell brings with her more than 10 years of experience in Internet policy issues, both from the legal and the technical side. Ms. Mitchell was the Director of Legal and Public Affairs for Mail Abuse Prevention Systems (MAPS), the original anti-spam company. Following her time at MAPS, Mitchell was co-founder and CEO of HABEAS. In her capacity at the Institute, Mitchell is involved with Internet issues ranging from email deliverability to spam and identity theft, cyber bullying, and everything in between. She has advised state officials at the highest levels and authored part of the federal anti-spam law. Ms. Mitchell is a graduate of Stanford Law School, sits on the advisory boards of several email and Internet security companies, and is on the faculty at Lincoln Law School.

Denise Olrich, a partner at Welch & Olrich, LLP, is a business attorney specializing in the legal needs of the entrepreneur, including e-commerce, privacy and cyberlaw matters, intellectual property matters, trademark registration, business formation, corporations and partnerships, business transactions, bankruptcy and bankruptcy litigation, as well as business litigation in the state courts. Ms. Olrich regularly lectures to attorneys, business groups, and students regarding business and cyberspace law matters and is the author of the chapter on *Internet and Electronic Privacy* in PRIVACY COMPLIANCE AND LITIGATION (Cal CEB 2008). She served on the committee that drafted California's new revised limited partnership law. She is a member of the California State Bar Business Law Section Executive Committee and is a past chair of both the Cyberspace Law Committee and the Partnerships and Limited Liability Companies Committee. Ms. Olrich received a B.A. from Michigan State University and a J.D. from Thomas M. Cooley Law School in Lansing, Michigan.

Nicole Ozer is the Technology and Civil Liberties Policy Director at the ACLU of Northern California, working on the intersection of new technology, privacy, and free speech. Nicole graduated magna cum laude from Amherst College, studied comparative civil rights history at the University of Cape Town, South Africa, and earned her J.D. with a Certificate in Law and Technology from Boalt Hall School of Law, University of California Berkeley. Before joining the ACLU, Nicole was an attorney at Morrison & Foerster LLP. Nicole was recognized by San Jose Magazine in 2001 for being one of 20 "Women Making a Mark" in Silicon Valley. Nicole's law review articles, policy publications, and regular blog posts are available at www.aclunc.org/tech.

Jefferson F. Scher is a partner in the Intellectual Property Group of Carr & Ferrell LLP, Palo Alto and chairs the firm's Trademark Practice Group. Mr. Scher specializes in intellectual property and cyberlaw counseling and dispute management, with an emphasis on the protection and enforcement of trademarks and copyrights. He counsels a wide range of companies on maximizing protection of their intellectual property, and managing risks associated with the use of others' information and intellectual property. Mr. Scher also is a lecturer at the Santa Clara University School of Law, where he teaches Trademarks and Unfair Competition.

Andrew B. Serwin is the founding chair of the Privacy, Security, and Information Management Practice and is a partner in the San Diego office of Foley & Lardner LLP. He is also co-chair of Foley's Privacy Litigation Task Force. Mr. Serwin has extensive experience in privacy and security matters, including state, federal and international restrictions on the use and transfer of information, compliance with FTC consent decrees, behavioral advertising, security breach compliance, EHR/PHR concerns, incident response, marketing restrictions, the drafting and implementation of privacy and security policies, content monitoring, as well as data transfers in the context of M&A and technology transactions. Mr. Serwin also advises media and Internet companies regarding online contracting issues, licensing issues, domain name issues, and intellectual property issues, as well as litigation resulting from information security incidents. Mr. Serwin has unique experience in representing start-up and Internet companies because he served as President and General Counsel of an online political magazine, InPolitics.com.

Mr. Serwin was recently named to Security Magazine's "25 Most Influential Industry Thought Leaders" for 2009, and is the only law firm lawyer to receive this award. He is ranked by Chambers USA – 2009 in the area of National: Privacy & Data Security, where he was described by clients as "*a tireless worker, holding onto the ever-shifting puzzle pieces of the law in this area in a way that other privacy lawyers cannot.*" He is also the author of INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE, which has been called "*the best privacy sourcebook,*" "*an indispensible resource for privacy professionals at all levels,*" and "*a book that everybody in the information privacy field should have on their desk,*" as well as INFORMATION SECURITY AND PRIVACY: A GUIDE TO INTERNATIONAL LAW AND COMPLIANCE. Mr. Serwin is also the author of the INTERNET MARKETING LAW HANDBOOK, also published by Thomson-West, which covers topics such as privacy and security, commercial email laws, spyware and unfair competition law. In addition, he has written *Poised on the Precipice: A Critical Examination of Privacy Litigation*, which was selected for publication by the Santa Clara Computer and High Technology Journal, and *Privacy 3.0 – The Principle of Proportionality*, accepted for publication by the University of Michigan Journal of Law Reform. He has written over 70 articles and presented over 90 times on litigation and privacy topics.

Mr. Serwin is the former Co-Chair of the California State Bar's Cyberspace Law Committee, and the former chair of the San Diego County Bar Association's website Committee from 2002-2004. Mr. Serwin also serves on the editorial board of Thomson-West's Cyberspace Lawyer, as well as the Privacy and Information Law Report. He is also a member of the Publications Board of the Business Law Section of the American Bar Association. Mr. Serwin serves on the Privacy Steering Committee and Red Flags Task Force for a major utility, is a member of the RIM Council of the Ponemon Institute, LLC, a group that brings together information management professionals from privacy and data protection disciplines to develop solutions to challenges facing an organization's acquisition, use, storage, transfer and disposal of information assets.

J. Anthony Vittal is the principal at The Vittal Law Firm in Los Angeles. After a career handling complex business litigation and conducting legislative advocacy on justice system issues, Mr. Vittal served as EVP/General Counsel of Credit.com, Inc. and as founding General Counsel of Identity Theft 911, LLC, in San Francisco. Since returning to private practice in Los Angeles, his practice also focuses on issues of Internet law, e-commerce, data security, and privacy. He currently serves as Co-Vice Chair of the Cyberspace Law Committee of the Business Law Section of the State Bar of California, Chair of the Law & Technology Committee of the ABA Tort Trial & Insurance Practice Section, Chair of the Technology Committee of the ABA General Practice Solo & Small Firm Division, and is a member of the editorial board of the Technology and Practice Guide issues of GP|Solo magazine, published by the Division. He also is a member of the Cyberspace Law Committee of the Business Law Section of the American Bar Association, various technology-related committees of the ABA Science & Technology Law Section and the ABA Antitrust Law Section, and the Information Systems Security Association. Mr. Vittal is a past president of the Beverly Hills Bar Association, a co-founder, and past president of the California Association of Local Bars, and a co-founder and past co-chair of the California Bench-Bar Coalition. He received his B.A. from Stanford University, did graduate work in artificial intelligence at UC Irvine, and received his JD from UCLA. He writes and lectures extensively on technology-related issues for lawyers.