

Information Technology Law 2008 in Review

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
New York
212.735.2750
stuart.levi@skadden.com

Rita Rodin Johnston
New York
212.735.3774
rita.rodin@skadden.com

Jose A. Esteves
New York
212.735.2948
jose.esteves@skadden.com

* * *

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

WWW.SKADDEN.COM

The Information Technology and E-Commerce Group at Skadden, Arps is pleased to provide this overview of what we believe were the key developments in technology law in 2008. As you will see, 2008 marked a critical juncture in the evolution of technology law, with courts handing down important decisions in a number of areas that previously had not been addressed. As always, we welcome your comments and input.

Content

Expectations of Privacy and Online Activity	1
Developments in Identity Theft Protection and Data Breach Notification Laws	4
The Enforceability of Electronic Agreements	8
Search Engine Caching and Copyright Infringement	10
Liability for Hosting Counterfeit Sales	11
Enforceability of Open Source Licenses	13
The Impact of the First Sale Doctrine on Shrinkwrap Licenses	15
Use of Trademarks in Video Games and Virtual Worlds	17
Liability for Third-Party Content and CDA Immunity	18
ICANN Announces Plan to Expand Domain Name Space	20

Expectations of Privacy and Online Activity

Just as the use of the Internet, social networking and other forms of electronic communication has exploded, so too have the legal developments that surround them, particularly the developments related to privacy. Over the past few years, courts have grappled with the appropriate level of privacy that users can expect when they transmit or post information via the Internet. This year was no exception as the courts addressed the expectation of privacy surrounding records of Internet activity, employee text messages and postings on social networks.

Access to ISP Records: *State v. Reid*

A unanimous decision by the New Jersey Supreme Court in April 2008 addressed the expectation of privacy that a user has in information stored by the individual's Internet service provider (ISP) regarding her Internet activity. In *State v. Reid*,¹ the defendant Reid used her home computer to log onto the Web site of a company that supplied materials to her employer's business. While on the supplier's Web site, Reid changed her employer's login and shipping address, without authorization. The supplier's Web site captured the 10-digit IP address of the user that had changed the employer's

¹ 194 N.J. 386 (2008)

information, and informed Reid's employer.² The municipal court issued a subpoena to the ISP, which revealed the subscriber information associated with the IP address, including Reid's name, address, telephone number, type of service provided, e-mail address and method of payment.

The trial court granted Reid's motion to suppress the evidence obtained via the municipal court subpoena. The court concluded that the subpoena violated Reid's expectation of privacy and was unconstitutional. The Appellate Division affirmed the order of suppression, reasoning that the state recognizes a right in "informational privacy, which encompasses any information that is identifiable to an individual."

The New Jersey Supreme Court agreed with the lower courts and held that citizens have a reasonable expectation of privacy in the subscriber information they provide to ISPs. Under the ruling, prosecutors can obtain ISP records only by serving a grand jury subpoena on a user's ISP. This court is the first to recognize a reasonable expectation of privacy associated with anonymous Internet use. The court's decision is more protective of privacy rights than the federal courts, which have not yet extended privacy rights to cover Internet subscriber information.

Access to Employee Text Messages: *Quon v. Arch Wireless Operating Co, Inc.*

Employer monitoring of employee communications continues to be rife with privacy issues. In June 2008, the U.S. Court of Appeals for the Ninth Circuit interpreted the Stored Communications Act (SCA)³ in the context of employee text messaging. The SCA prohibits an electronic communications service from disclosing the content of electronically stored messages to a subscriber unless the subscriber is also a sender or intended recipient of the message.

In *Quon v. Arch Wireless Operating Co., Inc.*,⁴ police officers were given two-way pagers to use in the scope of their employment. The department's contract with Arch Wireless provided that each pager would be allotted 25,000 characters per month for text messages. When an officer went over his allotted number of characters per month on the pager, he was required to pay overage charges. Although the department had a policy of monitoring e-mail and other forms of communication, the policy did not explicitly cover text messaging. A superior told the officers that if they paid the overage charges, their text messages would not be audited.

After various officers repeatedly went over their allotted characters, the police department conducted an audit to determine if the messages were exclusively work related, thereby requiring an increase in the number of characters permitted. Since the police department paid for the devices, it was considered to be the "subscriber" under the plan and was therefore able to obtain the archived messages from Arch Wireless. The department discovered that many of the messages were personal messages that were often sexually explicit.

The officers filed a complaint in the District Court for the Central District of California, alleging violations of the SCA and the Fourth Amendment. The district court held that Arch Wireless did not violate the SCA. The court explained that Arch Wireless was not a conduit for the transmission of

² An IP address is the numeric identifier assigned to each visitor of the Web site.

³ 18 U.S.C. §§ 2701-2711

⁴ 529 F.3d 892 (9th Cir. 2008)

communications that fit the definition of “electronic communications service,” but rather a “remote computing service,” or receptacle for communications. Therefore Arch Wireless committed no harm when it released the text-message transcripts to its “subscriber,” the city police department, although it was not a sender or intended recipient of the messages.

Additionally, the district court found that, in light of the informal policy that messages would not be audited, the officers had a reasonable expectation of privacy in their messages. The court concluded the search was reasonable, however, because the intent was to determine the efficacy of the character limit, not to uncover misconduct.

The Ninth Circuit reversed the district court decision and held that the SCA prohibits third-party service providers, such as Arch Wireless, from disclosing stored electronic communications without the consent of the employee who sends or receives the communication, even if the employer provides the equipment and pays for the service. Unlike the district court, the Ninth Circuit found that Arch Wireless was an electronic communications service.

The Ninth Circuit also noted that the officers had a reasonable expectation of privacy in their messages under the Fourth Amendment because a superior told the officers that their text messages would not be audited, even though the officers had signed an Internet policy stating that computer usage could be monitored. In conclusion, the Ninth Circuit held that the police department’s review of the text messages was an unreasonable search, regardless of the intent of the search.

Although this is an important decision in relation to third-party servers, it does not restrict an employer’s ability to monitor messages sent via a company-issued personal digital assistant, such as a BlackBerry, over the company’s own network, and not stored on a third-party server.

Information Disclosed on Social Network Sites: *Sandler v. Calcagni*

As more and more people join social networks and virtual communities, those communities and the courts increasingly question whether individuals who post personal information on publicly available Web sites have a reasonable expectation of privacy in their identity. In July 2008, the District Court of Maine weighed in on this issue. In *Sandler v. Calcagni*,⁵ a dispute between two high school classmates escalated into petty criminal charges against one of the students. After the students entered college, the parents of the student who was charged wrote a book about the dispute to tell their side of the story. The book contained private information about the other student, who subsequently filed suit against the parents and the printing company for defamation and privacy torts.

The district court ruled that the student’s invasion of privacy claim was negated by her own posting of the claimed private information on her publicly accessible MySpace page. The court noted that because the plaintiff had admitted on MySpace that she had sought psychological help, that fact was not only public, but her admission of it on MySpace established that she did not consider disclosure of the fact to be highly offensive. Accordingly, individuals who post private details about their lives on publicly accessible Web sites may not be able to successfully bring claims based on an expectation of privacy in those details.

5 2008 U.S. Dist. LEXIS 54374 (D. Me. July 16, 2008)

Impact

The foregoing cases highlight the complex legal issues related to Internet privacy. More frequently, courts are finding that individuals have a reasonable expectation of privacy in electronic communications as well as in the user information related to those communications. Going forward, companies may face challenges in obtaining information about an individual's Internet activity or an employee's electronic communications. Nonetheless, at least one court has recognized the public nature of the Internet and will not allow a user to publicly post information while at the same time claiming that information to be private.

Developments in Identity Theft Protection and Data Breach Notification Laws

This past year saw an increase in regulations aimed at detecting and combating consumer identity theft. At the federal level, the "Red Flag Rules" require certain companies to establish written programs to detect and respond to identity theft. At the state level, Massachusetts now requires a similar written information security program related to its residents' personal information, while a Nevada law requires the encryption of such personal information.

The FTC "Red Flag" Rules

On January 1, 2008, federal regulations aimed at preventing and combating identify theft went into effect. These "Red Flag Rules" were promulgated by the Federal Trade Commission (FTC), the federal banking regulatory agencies and the National Credit Union Administration (NCUA) pursuant to Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.⁶ The compliance deadline was November 1, 2008, although the FTC recently delayed its enforcement of the Rules until May 1, 2009. This delay, however, does not effect enforcement by the other regulatory authorities.

The Red Flag Rules apply to financial institutions and creditors that hold or maintain covered accounts, defined as accounts that are primarily used for personal, family or household purposes and involve multiple payments or transactions, such as a mortgage loan or cell phone accounts, or accounts for which there is a foreseeable risk of identity theft, such as a small business or sole proprietorship account. Financial institutions are defined in accordance with the Fair Credit Reporting Act and include banks, savings and loan associations, mutual savings banks and credit unions. Creditors are defined as persons or entities that regularly arrange for the extension, renewal or continuation of credit such as car dealers, utilities, telecommunications companies and other entities that defer payment for goods or services.

Generally, the Rules require financial institutions and creditors to develop a written program both identifying and detecting warning signs — the "red flags" — of identity theft and establishing appropriate responses to such red flags. The Rules give businesses significant flexibility, provided that they establish programs appropriate in light of their size, complexity, nature and scope of activities. Additionally, the program must be well-documented, updated periodically and overseen by the board of directors, a board committee or senior management-level employee.

To assist with program development, the Rules provide an extensive list of potential red flags to be reviewed by companies, which are organized into the following major categories:

⁶ See 12 C.F.R. §§ 12, 222, 334, 364, 571, 717 (2008); 16 C.F.R. § 681 (2008)

- alerts, notifications or warnings from consumer reporting agencies;
- the presentation of suspicious documents;
- the presentation of suspicious personal identifying information, such as a suspicious address change;
- unusual use of, or suspicious activity related to, a covered account, such as use in a manner inconsistent with established patterns of account activity; and
- notices from customers, identity theft victims, law enforcement authorities or other persons regarding potential identity theft related to covered accounts.

Additionally, the Special Rules for Card Issuers and the Address Discrepancy Rules require financial institutions and creditors who issue debit and credit cards or use consumer reports, including credit reports, to implement reasonable policies and procedures to assess the validity of address change requests. For example, these Rules are triggered when a card issuer receives an additional or replacement card request shortly after receiving an address change notification for the same account, or when a consumer report is requested for an individual at one address but the report's user is advised that the related individual resides at a substantially different address.

Massachusetts Enacts Broad Privacy Regulations

On September 19, 2008, Massachusetts issued the Standards for the Protection of Personal Information of Residents of the Commonwealth, governing the handling of state residents' personal information.⁷ The general compliance deadline was recently extended from January 1, 2009 to May 1, 2009.

The regulations apply widely to persons and entities that own, license, store or maintain personal information about any Massachusetts resident. "Personal information" is defined as a person's name combined with private information, such as a Social Security number, driver's license or any information that would permit access to a financial account.

The regulations create a duty to develop, implement, maintain and monitor a comprehensive, written information security program applicable to records containing residents' personal information that is "reasonably consistent with industry standards." Program sufficiency is evaluated by considering the size, scope and type of business, the amount of resources available, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. Every security program must include the following steps with respect to records that contain a resident's personal information:

- designate one or more employees to maintain the program;
- identify paper, electronic and other records; computer systems; and storage media, including laptops and portable media, that contain personal information;

⁷ 201 MASS. CODE REGS. 17.00 (2008)

- identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of such records;
- develop security policies addressing whether and how employees keep, access and transport such records outside business premises;
- prevent terminated employees from accessing such records;
- impose disciplinary measures for violations of the program's rules;
- take reasonable steps to verify that third-party service providers with access to such records have the capacity to protect the personal information;
- limit the amount of personal information collected, retained and accessed to that reasonably necessary to accomplish the legitimate purpose for which it is collected;
- reasonably restrict physical access to such records;
- regularly monitor and upgrade the information safeguards;
- review the program annually or after a material change in business practices; and
- document responsive actions and engage in mandatory post-incident review of events and actions taken.

Finally, the regulations impose specific requirements for establishing and maintaining a security system for computers, networks and other electronic systems that includes:

- secure user authentication protocols such as controlling user IDs and data security passwords and restricting access to active users only;
- secure access control measures that restrict access to records containing personal information and assign unique identifications plus passwords to persons with such access, reasonably designed to maintain the security system's integrity;
- encryption of records containing personal information that travels across public networks, wirelessly or are stored on laptops or portable devices, to the extent technically feasible;
- reasonable monitoring of systems for unauthorized access;
- reasonably up-to-date firewall protections and system security software, including malware protection and current patches and virus definitions; and
- education and training of employees on the security system's use.

Nevada Enacts Data Encryption Law

A Nevada law requiring encryption of customer personal information went into effect on October 1, 2008, bolstering existing state data security laws regarding the protection of personal information. Specifically, the new law provides that “a business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”⁸

“Personal information” is a person’s first name or first initial and last name combined with a Social Security number, driver’s license or identification card number or an account, credit or debit card number and its access code or password, but excludes the last four digits of a Social Security number or other publicly available information lawfully made public.⁹

“Encryption” is defined as “the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to: prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; cause or make any data, information, program, signal or sound unintelligible or unusable; or prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network.”¹⁰

While businesses have broad latitude under this definition, other industry standards may require stronger encryption technologies and should be considered when assessing whether a chosen encryption technology complies with the law. For example, the Payment Card Industry Data Security Standards (PCI DSS) require “strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) and Internet protocol security (IPSEC)” when transmitting sensitive cardholder data over open, public networks.

The Nevada law does not, however, define the terms “customer,” “electronic transmission” or “business in the State.” Under Nevada case law, whether a company is “doing business” in the state is a factual inquiry based upon the nature and quantity of its business. While the precise scope of “electronic transmission” also remains unclear, the term almost certainly encompasses e-mails. Finally, no enforcement measures are identified in the new law, although businesses should be aware that the law could be the basis for the duty of care standard in negligence suits alleging a failure to protect customer information.

Impact

In many instances, compliance with the above regulations will not require businesses to take significant new actions, as existing policies and procedures may address many of the requirements. However, businesses covered by these laws should coordinate their legal, business and technology teams to ensure compliance with applicable federal and state laws.

8 NEV. REV. STAT. § 597.970 (2008)

9 *Id.* § 603A.040

10 *Id.* § 205.4742

The Enforceability of Electronic Agreements

With the business world becoming increasingly digitized, electronic agreements and contracts continue to multiply. Although electronic contracts and electronic signatures have been recognized by federal and state governments, the courts have been forced to wrestle with many fundamental aspects of contract law when a dispute arises. This year, courts made important decisions regarding the enforceability of an offer and acceptance conducted by e-mail; the applicability of the Uniform Electronic Transaction Act (UETA) to contract formation; and the enforceability of online agreements that allow modification without notice.

Offer and Acceptance via Email: *Stevens v. Publicis*

Courts have frequently held that e-mail correspondence can qualify as a valid and enforceable agreement if certain elements are present. In April 2008, a New York Appellate Division court held that parties to a written contract may amend that contract via exchanges of e-mail messages, provided that the e-mails clearly detail the modifications and clearly express all parties' unqualified acceptance of the modifications.

In *Stevens v. Publicis, S.A.*,¹¹ after Stevens was removed from his post as CEO of Publicis-Dialog, he and Bloom, former chairman and CEO of Publicis USA, exchanged a series of e-mails regarding Stevens' new role at Publicis. Bloom sent Stevens an e-mail suggesting that Stevens could remain at Publicis if he spent 70 percent of his time developing business and the remainder cultivating former clients and managing operations. The next day, Stevens e-mailed his acceptance of the proposal, and Bloom responded to Stevens' e-mail, expressing his enthusiasm over Stevens' decision. When Stevens was subsequently not retained, he filed for breach of contract.

The New York County Supreme Court denied Stevens' motion for partial summary judgment on the grounds that the parties had agreed in writing to modify plaintiff's duties under the employment agreement. Stevens appealed the decision. The appellate court agreed with the lower court and ruled that the e-mail transactions fulfilled a clause in Stevens' existing employment agreement that obligated all parties to sign any modification to the agreement. The court held that the series of e-mails beginning with Bloom's message setting forth the terms of the proposed modification, together with Stevens' acceptance of the agreement and Bloom's immediate reply, memorialized the terms of the parties' agreement to change Stevens' responsibilities under the employment agreement. The court reasoned that the e-mails constituted "signed writings" under the statute of frauds because each e-mail bore the typed name of the sender at the foot of the message, which signaled the author's "intent to authenticate" its contents.

In light of this decision, businesses should review the provisions in their agreements that address the way in which those agreements can be amended. Specifically, standard contract clauses requiring that amendments be in writing will need to specify that e-mails with a typed name and/or signature block do not amount to a signed writing if a business wishes to exclude email modifications.

¹¹ 2008 N.Y. Slip Op. 02880

Application of the UETA to E-Mail Agreements: *Alliance Laundry Systems, LLC v. Thyssenkrupp Materials*

In 1999, the Uniform Electronic Transactions Act (UETA) was adopted by the National Conference of Commissioners on Uniform State Laws in an effort to ensure the enforceability of electronic signatures and communications in business and commercial transactions. In 2008, *Alliance Laundry Systems, LLC v. Thyssenkrupp Materials, NA*¹² addressed a fundamental issue regarding the application of the UETA to the formation of a contract by e-mail exchange.

Alliance involves a plaintiff buyer and a defendant steel company that negotiated terms of a proposed transaction over e-mail. When the steel company failed to deliver the steel as the buyer expected, the buyer sued, asserting that a contract was formed by the e-mail exchange. The district court denied the plaintiff's motion for summary judgment on the grounds that there was a genuine issue regarding contract formation.

In its opinion, the court addressed the defendant's argument that the e-mail exchange did not result in the formation of a contract because under the UETA, parties cannot form a contract electronically unless they first make an agreement to do so. The court concluded, however, that Article 2 of the Uniform Commercial Code (UCC), which requires that a contract for the sale of goods priced at \$500 or more be evidenced by a writing signed by the party against whom enforcement is sought, provides the substantive law that determines whether parties form a contract.

The court, citing the Prefatory Note to the UETA, further explained that the purpose of the UETA was to validate the use of electronic records and signatures, not to create a general contracting statute. Therefore, if the evidence shows that the parties "reached an agreement electronically, it will likely also show that the parties agreed to conduct the transaction by electronic means." In other words, if the jury finds that by negotiating the proposed transaction over e-mail the parties intended to enter into a binding agreement under the UCC, then an electronic signature is valid under the UETA and thereby fulfills the UCC signature requirement.

The court's ruling clarifies the distinction between the applicability of the UCC to contract formation and of UETA to the enforceability of electronic signatures. Parties seeking to enter into electronic agreements should ensure that they are meeting the requirements for a signed writing under the UCC, and look to the UETA only as it concerns the validity of the electronic signatures to such agreement in order to fulfill such requirements.

Modifying Online Agreements Without Notice: *Margae v. Clear Link Technologies, LLC*

Courts have typically refused to enforce agreements between a consumer and a commercial party where the commercial party has the right to modify the terms without notice, simply by posting the modified terms on its Web site. In June 2008, the District Court of Utah considered such a situation where both parties were commercial entities.

*Margae v. Clear Link Technologies, LLC*¹³ involved two commercial parties that entered into an oral agreement under which Margae would provide affiliate marketing and search engine optimization

¹² 2008 U.S. Dist. LEXIS 58985 (E.D. Wisc. Aug. 5, 2008)

¹³ 2008 U.S. Dist. LEXIS 46765 (D. Utah, June 16, 2008)

services to Clear Link. Margae's principal representative assented to an agreement covering these services on Clear Link's Web site by clicking on a link stating "I accept these terms." The agreement allowed Clear Link to modify it at any time by notifying Margae or by posting a new agreement on Clear Link's Web site. The agreement further stated that if Margae continued to provide services under the new terms, it would be deemed to have accepted the modification. In June 2006, Clear Link posted a new agreement on its Web site. Unlike the original agreement, the modified agreement contained an arbitration provision.

When the parties had a disagreement about the work Margae had performed, Clear Link refused to pay Margae. Subsequently, Margae filed suit against Clear Link. Relying on the arbitration provision in the modified agreement, Clear Link sought to compel arbitration of Margae's claims against Clear Link. Margae opposed Clear Link's motion to compel arbitration on the grounds that the modified agreement was unenforceable because the provision allowing Clear Link to modify the terms without notice was unconscionable.

The district court held that the provision allowing for modification without notice was not unconscionable, and therefore the modified agreement was enforceable. The court pointed out that, pursuant to the original agreement, Margae agreed to be bound by modifications posted on Clear Link's Web site, whether it received notice or not. Additionally, the court found that neither the original agreement nor the modified agreement were procedurally or substantively unconscionable. The court relied on the fact that both parties were sophisticated, "Internet-savvy" corporations that entered into a contract on the Internet and agreed to make changes through the Internet.

The court's ruling reaches a markedly different conclusion from past cases involving online agreements between an individual and a commercial company. The decision sets forth a new precedent for commercial parties that enter into online agreements with "no notice" modification provisions. Companies entering into these types of agreements should review them carefully to determine whether they are willing to be bound by these types of terms.

Impact

Electronic communications are playing an increasingly important role in today's business world, particularly in relation to negotiating and consummating agreements. Parties must therefore proceed with caution when transacting electronically and should determine from the outset the circumstances under which an electronic communication or signature will be binding.

Search Engine Caching and Copyright Infringement

Search engines routinely use crawling and caching to create an index of Web pages and to allow user to find and retrieve pages more quickly. When a user conducts a search on a search engine, such as Yahoo! or Google, the index provides rapid search results including hyperlinks to the archived, or cached, copies of the Web pages matching the user's inquiry. Although most Web sites want their content to be indexed and available on search engines, those that do not may opt-out by sending a take-down notice to the search engine or by employing an electronic "robots.txt" protocol. The latter is a file placed on a Web site operator's server that tells search engine spiders not to crawl or index certain sections or pages of the site.

In September 2008, the District Court for the Eastern District of Pennsylvania held that a Web site operator's failure to deploy a robots.txt file gave rise to an implied license for search engines to index the site. In *Parker v. Yahoo!, Inc.*,¹⁴ Parker, a Web site operator, claimed that by making cached copies of his Web sites available to its users, Yahoo! infringed his copyright because it republished his works in their entirety without permission. Parker conceded that he deliberately chose not to use the robots.txt file on his Web site, but argued that he provided constructive notice to the defendants that he did not grant a license to cache his Web site by registering the copyright in his works and including a copyright notice on his Web site.

The court dismissed Parker's constructive notice argument on the grounds that he engaged in conduct from which Yahoo could properly infer that Parker consented to the use of his material in Yahoo's index. Specifically, Parker's deliberate decision not to use a robots.txt file was conclusive on the issue of an implied license to cache his Web site.

However, the court did not dismiss plaintiff's complaint in its entirety. The court noted that a nonexclusive implied license can be revoked where no consideration has been given for the license. The court further recognized that the initiation of a lawsuit itself may constitute such revocation of an implied license. Therefore, Yahoo's continued caching of Parker's works might constitute copyright infringement.

Impact

The court's ruling left open the proposition that a search engine *may* be liable for infringement once it knows or should know that it no longer has permission to display the cached content. For the most part, however, the decision further legitimizes search engine practices through the recognition of an implied license to crawl and cache in order to make content easily searchable by Internet users.

Liability for Hosting Counterfeit Sales

With the increasing role of online marketplaces in facilitating high volume sales transactions, questions surrounding the liability of host Web sites have become increasingly important. In *Tiffany, Inc. v. eBay, Inc.*,¹⁵ the District Court for the Southern District of New York addressed the contributory liability of an online auction Web site for intellectual property infringement.

Through its electronic marketplace, eBay facilitates transactions between two independent parties; it is not a retailer and it does not take physical possession of the goods sold. eBay requires those who trade on its Web site to sign its user agreement, which obligates users to refrain from violating any laws, third-party rights (including intellectual property rights) and eBay policies.

Given the potential for traders to sell fraudulent or infringing goods on its Web site, eBay has made substantial investments in anti-counterfeiting initiatives. The eBay "fraud engine" uses rules and complex models that automatically search for activity that violates eBay policies. The fraud engine monitors the Web site and flags or removes listings that, among other things, explicitly offer counterfeit items, contain blatant disclaimers of genuineness or include statements that the seller cannot guarantee the authenticity of the items. In addition, eBay has implemented the Verified

14 2008 U.S. Dist. LEXIS 74512 (E.D. Pa., Sept. 25, 2008)

15 576 F. Supp. 2d 463 (S.D.N.Y. 2008)

Rights Owner (VeRO) Program to address listings that offer potentially infringing items. Under the VeRO Program, owners can report such a listing by submitting a Notice of Claimed Infringement (NOCI) form, so that eBay can remove such reported listing.

On May 14, 2003, Tiffany's outside counsel wrote to eBay to complain about the "deluge" of counterfeit Tiffany jewelry on eBay. In its letter, Tiffany demanded, among other things, that eBay immediately remove listings for all Tiffany counterfeit merchandise on eBay's Web site. Tiffany also advised eBay that because there were no authorized third-party vendors for Tiffany merchandise, it should be apparent to eBay that any seller of five pieces or more of purported "Tiffany" jewelry was almost certainly selling counterfeit merchandise. When eBay rejected Tiffany's request for such a prospective ban, Tiffany filed suit against eBay.

Tiffany alleged that eBay was liable for contributory trademark infringement, on the grounds that eBay facilitated and allowed the counterfeit items to be sold on its Web site. Contributory trademark infringement occurs when: (1) one intentionally induces another to infringe on a trademark or (2) continues to supply a product knowing that one's customer is using it to engage in trademark infringement.¹⁶ To determine whether the defendant is liable for contributory trademark infringement under the "supply" prong, courts must analyze whether the defendant had the ability to supervise and control the means of infringement and whether it knew or should have known of the infringement.

The court first held that the eBay marketplace was a "product" that customers were using to engage in trademark infringement. The court's holding followed decisions in the Seventh and Ninth Circuits¹⁷ that held that a marketplace in which substantial quantities of infringing goods were sold met the definition of a "product" under the "supply" prong.

The court then analyzed the knowledge requirement. The court found that the demand letters sent by Tiffany to eBay along with thousands of NOCI forms alleging a good faith belief that certain listings infringed on Tiffany trademarks, all demonstrated that eBay only had "generalized" knowledge of the potentially infringing activity. Such knowledge is not sufficient to create liability for contributory infringement. The court stressed that to prove contributory trademark infringement, the plaintiff must prove the defendant knew or had reason to know of specific infringement by the seller.

The court dismissed Tiffany's argument that it satisfied the specificity requirement through the letters it sent to eBay in which it provided detailed notice of the problem and requested that all listings with five or more Tiffany items be removed. The court held that there was little support for the notion that the "five-or-more rule" presumptively demonstrated the presence of infringing items, and that "eBay was under no obligation to credit the potentially self-serving assertions of a trademark owner, particularly when those assertions — such as the 'five-or-more' rule — were unfounded."

The court next addressed Tiffany's argument that eBay could have taken any number of steps to further investigate the counterfeit sales, and that eBay's failure to do so constituted willful blindness, which satisfies the "reason to know" standard. The court concluded that eBay was not willfully blind, emphasizing eBay's anti-fraud measures. The policing efforts employed by eBay convinced the court that the Web site was not trying to avoid knowledge of counterfeiting activity, but rather was seeking to eliminate that activity.

¹⁶ *Inwood Laboratories Inc. v. Ives Laboratories Inc.*, 456 U.S. 844, 854-55 (1982)

¹⁷ *Hard Rock Cafe Licensing Corp. v. Concession Services Inc.*, 955 F.2d 1143 (7th Cir. 1992); *Fonavisa Inc. v. Cherry Auction Inc.*, 76 F.3d 259 (9th Cir. 1996)

Solely for the purpose of discussing the “continuing to supply” standard of contributory trademark infringement, the court assumed that the filing of a NOCI provided eBay with specific knowledge of infringement. The court noted that even if, for argument’s sake, this met the knowledge requirement, Tiffany still needed to show that eBay continued to supply its product to known infringers. The court noted that when Tiffany filed a NOCI, eBay’s practice was to promptly remove the challenged listing from its Web site. Additionally, eBay also warned sellers and buyers, cancelled all fees associated with the listing and directed buyers not to carry out the sale of the item. Accordingly, the court concluded that Tiffany failed to prove that eBay continued to supply its services in instances where it knew of infringement.

Finally, the court compared eBay’s anti-fraud efforts with Tiffany’s. The court found that Tiffany’s efforts at eliminating trademark infringement on eBay were relatively meager when compared to eBay’s efforts. The court rejected Tiffany’s assertion that eBay should bear the burden of identifying counterfeit goods because eBay was better able to screen potentially counterfeit listings than Tiffany. The court went so far as to say that, even if it were true that eBay was best situated to eliminate trademark infringement, “the fact remains that rights holders bear the principal responsibility to police their trademarks.”

Impact

The court’s ruling establishes that efforts to minimize misconduct can prevent liability for contributory trademark infringement. In addition, “general” knowledge of infringing activity is not sufficient to impute knowledge of any specific acts of infringement. Instead, the knowledge requirement will only be satisfied where an online marketplace knows or should know that specific listed items are infringing.

Enforceability of Open Source Licenses

Open source software licenses generally grant users broad rights to use, modify and distribute the software covered by the license. In many cases, the underlying source code for the software is also provided to facilitate the ability to make modifications. While these licenses have existed for a number of years, there has been some concern as to how they would be interpreted by courts. In August 2008, the U.S. Court of Appeals for the Federal Circuit issued an important decision holding that the violation of an open source license can be deemed copyright infringement despite the broad grant of rights offered by the open source license.¹⁸

The case, *Jacobsen v. Katzer*,¹⁹ involved an open source program, DecoderPro, that allowed model train hobbyists to program computer chips that control model trains. Jacobsen managed the open source group that created DecoderPro, and released the program under the Artistic License, an open source agreement that granted broad usage rights.

Katzer offered a competing product, Decoder Commander, that incorporated certain files from DecoderPro. Jacobsen argued that while using the files was permitted under the Artistic License,

¹⁸ Appeals concerning copyright law are rare in the Federal Circuit, which primarily handles patent cases. However, because the counterclaim in the case also sought to invalidate a patent issued to the plaintiff, the complaint arose, in part, under the patent laws, thereby granting the Federal Circuit proper appellate jurisdiction.

¹⁹ No. 2008-1001, 2008 WL 3395772 (Fed. Cir. Aug. 13, 2008)

Katzer had infringed the copyright in DecoderPro by not complying with certain attribution requirements of the Artistic License. Specifically, copies of the Katzer program did not include: the original author's name, the JMRI copyright notices, references to the Artistic License or an identification of JMRI as the original source of the definition files.

According to Jacobsen, Katzer's violation of the Artistic License constituted copyright infringement, which, upon the showing of a likelihood of success on the merits, created the presumption of irreparable harm that is necessary to support a preliminary injunction. Katzer argued that while he might be liable for breach of contract, he could not have engaged in copyright infringement given the broad grant of rights under the Artistic License. The U.S. District Court for the Northern District of California agreed with Katzer and denied Jacobsen's preliminary injunction motion.²⁰ Jacobsen appealed.

On appeal, the Federal Circuit noted that the key issue was whether the attribution requirements of the Artistic License were "covenants" or "conditions" of the license. If these requirements were merely covenants that were ancillary to the grant of the license, then Katzer had not infringed the copyright in the program, and was liable only for breach of contract. However, if the requirements were conditions of the license, then Katzer's failure to comply meant that he had failed to comply with the license grant itself, and was therefore liable for copyright infringement.

Katzer argued that the attribution requirements had to be mere covenants since Jacobsen had made his code publicly available at no charge. Since Jacobsen did not benefit from the license, then surely he could not have attached "conditions" to it. Katzer further argued that copyright law does not recognize a cause of action for non-economic rights, which were the only rights Jacobsen had in his open source program. Jacobsen countered that the terms of the Artistic License define the scope of the license and that any use outside of these restrictions constitutes copyright infringement.

The Federal Circuit agreed with Jacobsen and held that the attribution requirements were conditions of the license grant. The court noted that the wording of the Artistic License clearly states that its purpose is to create conditions, not covenants, to protect the rights of licensors: "The intent of this document is to state the conditions under which a Package may be copied." The Federal Circuit also noted that the Artistic License uses traditional language of conditions by stating that the right to copy, modify and/or distribute covered software is granted "provided that" certain attribution conditions are met. In the Federal Circuit's opinion, interpreting the attribution provisions of the Artistic License as mere covenants would render open source licenses "meaningless."

The Federal Circuit also addressed Katzer's argument that any benefit from an open source license was non-economic in nature. According to the court, the conditions created by the Artistic License are "vital to enable the copyright holder to retain the ability to benefit from the work of downstream users." Such downstream use provides the licensor with significant and direct economic benefit. For example, it allows the licensor to debug and improve programs faster through the contributions of others.

²⁰ No. C. 06-01905 JSW, 2007 WL 2358628 (N.D. Cal. Aug. 17, 2007)

Most importantly, in broad support of the open source approach to licensing the court stated:

The choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes, rather than as a dollar-denominated fee, is entitled to no less legal recognition.

Having found that copyright law was indeed applicable to Jacobsen's claim and that the terms of the Artistic License created conditions as to the scope of such license, the Federal Circuit vacated the district court's decision and remanded the case to determine whether Jacobsen had demonstrated a likelihood of success on the merits.

Impact

Although the decision in *Katzer* focused primarily on the language of the Artistic License, the Federal Circuit's holding on the economic benefit of open source licenses has broad applicability. Licensors of open source software now have some judicial support for the proposition that the nonmonetary benefits provided by an open source license are entitled to legal recognition.

The Impact of the First Sale Doctrine on Shrinkwrap Licenses

For years, software companies have relied on shrinkwrap license agreements to support the argument that transfers of packaged software to customers are licenses to use copies of the software, rather than sales of such copies. However, in *Vernor v. Autodesk*²¹, the Western District Court of Washington held that a plaintiff who purchased several copies of packaged software was the owner of those purchased copies, not merely a licensee, even though the use of the software was subject to a shrinkwrap license. As a result, the copies could be transferred to third parties without violating the software provider's copyright rights.

Background

Plaintiff Timothy Vernor purchased a copy of Autodesk software at a garage sale in 2005 and attempted to resell the software on eBay. Autodesk sent a Digital Millennium Copyright Act (DMCA) notice to eBay claiming a sale would infringe its copyright, and eBay suspended the auction. Vernor sent a DMCA counter-notice to which Autodesk did not respond, and eBay reinstated the auction. Vernor then sold the software to a third-party. In 2007, Vernor purchased additional copies of Autodesk software from an architectural firm, Cardwell/Thomas Associates (CTA), and four similar disputes between Vernor and Autodesk occurred when Vernor attempted to resell those additional copies. The first three disputes resulted in completed sales by Vernor, and the fourth resulted in eBay suspending Vernor's account for one month for repeat infringement complaints.

Vernor brought suit in the Western District Court of Washington, seeking a declaratory judgment that his reselling of Autodesk software was lawful under the first sale doctrine. The first sale doctrine permits a person who owns a legitimate copy of copyrighted material to sell or otherwise

²¹ Case No. C07-1189RAJ, W.D. Wash., May 20, 2008

dispose of that particular copy without violating the copyright holder's distribution rights.²² However, software providers have typically taken the position that providing a customer with a copy of the software in exchange for a one-time fee is merely a license of that copy to the customer and, as such, the customer does not own the copy, and the first sale doctrine does not apply. Autodesk accordingly argued that because CTA's use of the software was subject to a shrink-wrap license agreement, CTA was merely a licensee, not an owner, of the software copies, and neither CTA nor Vernor were protected by the first sale doctrine.

The Court's Decision

The *Vernor* court did not dispute Autodesk's assertion that licensees are not protected by the first sale doctrine. However, the *Vernor* court rejected Autodesk's position that the transfer of the software copies to CTA occurred pursuant to a license. Rather than relying on precedent holding that similar transfers did not constitute sales, but were instead licenses, the court in *Vernor* applied the reasoning of *United States v. Wise*.²³

The *Wise* case considered whether a movie studio's transfer of film prints to television networks and movie stars were sales or merely licenses. The *Wise* court made its decision on the basis of whether the transferees were allowed to keep the film prints (as opposed to having to eventually return the prints to the studio). Using this test, the *Wise* court found that sales of the prints had occurred even in transfers where the accompanying agreement contained draconian restrictions on resale. In these transfers, the first sale doctrine allowed the purchaser to resell the film prints without infringing the movie studio's copyright.

Using the *Wise* rationale, the *Vernor* court reasoned that because CTA was allowed to retain possession of the copies of Autodesk software in exchange for a single up-front payment, Autodesk's transfer of the copies to CTA constituted sales, not licenses, of such copies, even though such transfers occurred pursuant to license agreements that significantly restricted CTA's ability to resell the copies. Because CTA owned the copies, CTA's and then Vernor's subsequent sales were protected under the first sale doctrine (although Autodesk was not precluded from suing CTA for breach of contract of the license agreement).

In following *Wise*, the *Vernor* court explicitly rejected three later Ninth Circuit cases that upheld the principle that transfers of software copies pursuant to license agreements were not sales, but merely licenses.²⁴ The *Vernor* court reasoned that because the three earlier cases and *Wise* were all Ninth Circuit panel opinions (opinions decided by panels of three judges instead of the full court), in the case of a conflict among their holdings, the earliest case, *Wise*, must prevail. The *Vernor* court cited both Ninth and Fifth Circuit law that supported this method of resolving conflicts between panel opinions. However, it is notable that the *Vernor* court chose to base its decision on *Wise* because, unlike the three later cases, *Wise* was not a case about software.

²² 17 U.S.C. § 109(a)

²³ 550 F.2d 1180 (9th Cir. 1977)

²⁴ *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993); *Triad Sys. Corp. v. Southeastern Express Co.*, 64 F.3d 1330 (9th Cir. 1995); and *Wall Data Inc. v. Los Angeles County Sheriff's Dep't.*, 447 F.3d 769 (9th Cir. 2006)

Impact

In drafting license agreements, particularly those applicable to packaged software, software providers should consider whether they wish to prohibit subsequent sales of the software copies by their customers. If so, software providers should weigh the benefits of prohibiting such sales against the costs of restructuring the licensing programs for such software in a manner designed to avoid application of the first sale doctrine (such as requiring return of the software copies after a period of time, and/or a series of royalty payments over time).

Use of Trademarks in Video Games and Virtual Worlds: The Intersection Between Trademark Law and First Amendment Rights

In November 2008, the Ninth Circuit addressed the intersection between trademark law and the First Amendment. In *E.S.S. Entertainment 2000, Inc. v. Rock Star Videos, Inc.*, the court held that a defendant who used elements of the plaintiff's logo and trade dress in its video game was protected under the First Amendment.²⁵

Background

The plaintiff, E.S.S. Entertainment 2000, Inc., operates an East Los Angeles adult entertainment facility called the "Play Pen Gentlemen's Club." Defendant Rockstar Games, Inc. manufactures and distributes the "Grand Theft Auto" video game series. The game at issue, "Grand Theft Auto: San Andreas," is set in Los Santos a fictional, cartoon city that mimics the look and feel of Los Angeles. Game players travel throughout Los Santos, frequenting locations modeled after various real Los Angeles establishments. One such location, the East Los Santos "Pig Pen" club incorporates elements of plaintiff's Play Pen trade dress and logo.

The plaintiff alleged that that the virtual Pig Pen infringed its trademark and trade dress associated with the Play Pen, asserting claims under both the federal Lanham Act and state law. The defendant moved for summary judgment based on nominative fair use and First Amendment defenses. The federal district court granted the defendant's motion for summary judgment on the grounds that the defendant's use was protected under the First Amendment. The plaintiff appealed this decision.

The Court's Decision

The Ninth Circuit first rejected the defendant's nominative fair use argument. Nominative fair use protects one who deliberately uses another's trademark or trade dress for purposes of comparison, criticism, or point of reference. Because the defendant's Pig Pen was nonidentical to the Play Pen, it did not actually use the plaintiff's logo or trade dress and thus the defense was unavailable.

The Ninth Circuit did, however, affirm the district court's holding that the First Amendment barred the trademark and trade dress infringement claims. The Ninth Circuit applied a Second Circuit standard, construing the Lanham Act "to apply to artistic works only where the public interest in avoiding consumer confusion outweighs the public interest in free expression."²⁶ Under the *Rogers* test, the First Amendment protects use of a trademark if such use has some artistic relevance to the

²⁵ No. 06-56237 (9th Cir. Nov. 5, 2008)

²⁶ *Id.* (quoting *Rogers v. Grimaldi*, 875 F.2d 994, 999 (2d Cir. 1989))

underlying work and does not explicitly mislead as to the source or content of the work. Although the test traditionally applies to use of a trademark in the title of an artistic work, the Ninth Circuit extended its application to use in the body of a work.

The plaintiff conceded that the video game qualified as an artistic work. Applying *Rogers*, the Ninth Circuit first held that the video game did bear artistic relevance to the Play Pen club, despite the fact that the game was not “about” the Play Pen, noting that only a modicum of relevance is required under the *Rogers* test. The court found that the look and feel of the neighborhood including the Play Pen was relevant to the video game’s artistic goal of creating a “cartoon-style parody of East Los Angeles.”

Second, the Ninth Circuit found that the defendant’s use did not explicitly mislead as to the source or content of the work. The court noted that the video game and the Play Pen club shared little or nothing in common, and that the buying public would not have believed that plaintiff had produced or supported the video game. Because both prongs of the *Rogers* test were satisfied, the court affirmed that the defendant’s use of the Play Pen trade dress and trademark were protected by the First Amendment.

Impact

E.S.S. Entertainment expands the use of the *Rogers* test beyond the use of a mark in the title of an artistic work to cases where the mark is used in the body of the work. In this respect, the Ninth Circuit is treating such uses similar to a parody or spoof. This expanded protection for artistic works may pose concern for trade dress and trademark owners in an environment where video games and virtual worlds are making liberal unauthorized use of trademarks. Trademark owners will need to carefully monitor whether other courts follow the Ninth Circuit’s lead in this important area.

Liability for Third-Party Content: Interpreting the Immunity Granted by the Communications Decency Act

In 2008, both the Seventh and Ninth Circuits addressed the scope of immunity provided under the Communications Decency Act (CDA) for Web sites that post third-party content. Both of these cases — *Chicago Lawyers’ Committee for Civil Rights under Law, Inc. v. Craigslist, Inc.*²⁷ and *Fair Housing Council of San Fernando Valley v. Roommates.com*²⁸ — involved the intersection between the CDA and the Fair Housing Act (FHA).

Background to the CDA

The CDA provides immunity to certain providers of interactive computer services that publish third-party content.²⁹ Pursuant to the act, Web sites are immune from claims related to third-party content if they passively publish such content, even if such content is defamatory or otherwise contains illegal content. However, the CDA does not protect a site assuming a more active role as an

27 519 F.3d 666 (7th Cir. 2008)

28 521 F.3d 1157 (9th Cir. 2008)

29 47 U.S.C. § 230(c) (2006)

“information content provider,” defined as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet.”³⁰ A Web site operator can be both a service provider and a content provider.

Chicago Lawyers’ Committee for Civil Rights under Law, Inc. v. Craigslist, Inc.

In *Chicago Lawyers’ Committee for Civil Rights under Law, Inc. v. Craigslist, Inc.*, the plaintiff, a nonprofit public interest organization in Chicago, alleged that Craigslist had violated the FHA by including user postings that were discriminatory.³¹ The district court granted Craigslist’s motion to dismiss on the grounds that it had immunity under the CDA.

The Seventh Circuit affirmed, reasoning that Craigslist could not be liable under the FHA unless it “published” the discriminatory statements. Since, under the plain language of the CDA, an “online information system” such as Craigslist could not be treated as a “publisher or speaker” of third-party content, it was immune from FHA liability. The court further noted that nothing in the Craigslist service induced anyone to express discriminatory preferences or post discriminatory listings.

Fair Housing Council of San Fernando Valley v. Roommates.com

The Ninth Circuit took a different view in *Fair Housing Council of San Fernando Valley v. Roommates.com*. In 2004, two local Fair Housing Councils in California filed suit in federal district court alleging that Roommates.com, a site providing online, roommate matching services, had violated the FHA. The plaintiffs based their claim on the manner in which Roommates solicited information from users and the content that it allowed users to post on the site. Roommates asserted it was immune from liability under the CDA.

The district court agreed with Roommates and dismissed the claims without reaching the merits of the plaintiff’s FHA claim. The Ninth Circuit, however, reversed and held that Roommates was, in fact, a content provider because it actually created or helped develop the third-party information on its site.

The court first focused on the online questionnaires that users had to complete in order to become members of Roommates.com. These questionnaires featured drop-down menus which prompted users for their gender, sexual orientation and whether children would live in the household. Prospective members also completed a form indicating preferences for the types of individuals with whom they were willing, and not willing, to live. Because Roommates developed these forms and provided possible responses to choose from, the Ninth Circuit held that the site not a passive publisher of third-party information, but rather active in the creation and development of discriminatory content.

The court then addressed Roommates’ e-mail notifications and search functionalities. These notifications permitted subscribers to receive e-mails regarding housing opportunities that matched their profile, while the search functionality allowed users to base their searches on the preference and personal characteristic information that was gathered through the drop-down menus. The Ninth Circuit held that, because the search engine relied on the discriminatory criteria that the site had itself offered as choices, it was different from a generic search engine and therefore did not enjoy CDA protection.

³⁰ *Id.* § 230(f)(3)

³¹ The FHA prohibits discrimination on the basis of race, religion, sex or family status in connection with housing sales or rentals. The FHA also bans notices, statements or advertisements that make, print, publish or intend to make any such discrimination. 42 U.S.C. § 3604(a) (2006)

The court was careful to note that services, such as online dating Web sites, that prompt users to enter their race, sex and religion and then allow searches based on those criteria retained CDA immunity because “it is perfectly legal to discriminate along those lines in dating.”

The Ninth Circuit also analyzed the “additional comments” section that Roommates provided in each member’s profile, which allowed members to enter any text they desired. Ironically, while some of the most discriminatory comments were included in these comment section, the court found that this aspect of the site was entitled to CDA immunity. The court relied on the open-ended nature of the blank text box and the fact that Roommates did not use information provided in the additional comments to filter member profiles.

The dissent expressed deep concern regarding what it characterized as an “unprecedented” expansion of Web site liability. The dissent was also troubled that the majority had relied on the substance of the underlying FHA statute to determine whether Roommates should be immune under the CDA. According to the dissent, “[w]hether Roommates is entitled to immunity [under the CDA] from publishing and sorting profiles is wholly distinct from whether Roommates may be liable for violations of the FHA.”

Impact

Web sites have long taken comfort in the broad immunity provided by the CDA. While the Seventh Circuit reaffirms CDA protection for activities where a site had no active role in creating the third-party content published on the site, it is noteworthy that the Ninth Circuit found that seemingly innocuous activities, such as providing drop-down menus and filtering content, can be construed as publishing content. This narrow construction of CDA immunity can easily transform a “passive” Web site provider into an unprotected content provider. Web site providers need to evaluate their online functionality carefully to avoid taking any action that would satisfy the Ninth Circuit’s broad definition of “content provider.”

ICANN Announces Plan to Expand Domain Name Space — Opportunity for Some, Headache for Others

The coming year promises to be an exciting one in the domain name space. In June 2008, the Internet Corporation for Assigned Names and Numbers (ICANN), the organization responsible for coordinating domain name policy, announced a plan to significantly expand the domain name space by soliciting applications to create new generic top-level domains (gTLDs) (*e.g.*, .com, .org). ICANN followed up on this announcement in November by publishing a related Draft Applicant Guidebook for public review and comment which describes the application process in greater detail. The expansion of the domain name space offers companies seeking to create new gTLDs an opportunity for significant financial rewards, while simultaneously presenting a challenge to trademark owners seeking to protect their brands on the Internet.

Background

ICANN has offered companies the opportunity to apply for new top-level domains (TLDs) only twice before — in 2000 and in 2004. Each of these rounds was tightly controlled, with ICANN rejecting most applications for technical, financial or political reasons. As a result, out of nearly 60 applications received during these two prior rounds, ICANN approved only 13 new TLDs, including gTLDs such as .info and .biz and “sponsored” TLDs such as .jobs, .tel and .coop.

For this upcoming round, ICANN has announced that it expects to approve many more new gTLDs and will take a more “hands off” approach to its review and approval process. This approach should encourage many more applications since it reduces the risk that an applicant will spend significant time and resources to prepare an application, only to have it rejected by ICANN.

Timeline

ICANN has not announced an official timeline for the next round of gTLD applications, but it did indicate that it hoped to begin the process in the first quarter of 2009. However, recent communications from the U.S. Department of Commerce and various other organizations and groups urged ICANN to delay the process and take additional time to study issues such as the need for additional gTLDs, the risk of harm to consumers and whether ICANN is the appropriate body for resolving some of the complex moral and political issues that could be raised in the process. As of the end of 2008, however, ICANN had not announced whether it will comply with these requests.

Application Process³²

The new gTLD application process will be open to all companies that wish to apply, and that pay an application fee, which is currently planned to be \$185,000. Under the draft, applicants must demonstrate through the application process that they possess the financial and technical resources and expertise needed to operate the gTLD if their applications are successful. Applicants that fail to demonstrate that they have these resources will be rejected, though they will have an opportunity to appeal the initial rejection.

There will be no limits on what word or letters can be used to apply for a new gTLD (though they will be subject to challenge on various grounds, as described below), and for the first time, applicants will be allowed to apply for gTLDs using non-ASCII characters such as Cyrillic letters for Russian-language TLDs. Many expect the major Internet and technology companies to submit applications for their brands.

There also will be no requirement that a gTLD be used in the same manner as other existing gTLDs. So, for example, a company could apply for a .geo gTLD that uses domain names based on geographic coordinates (a similar application was unsuccessful in the 2000 gTLD round). In addition, applicants may identify their gTLDs as “community” gTLDs — which means they are identified as serving a defined community of users. As a result of the relatively few restrictions on applications, many expect this new round to include a variety of novel uses for gTLDs beyond simple domain names for Web sites and email.

ICANN will post all complete applications it receives for public review and comment. After the applications are posted, the public will have an opportunity to lodge objections to applications on one of four grounds: (1) the proposed gTLD is confusingly similar to an existing TLD; (2) the proposed gTLD infringes the intellectual property rights of others (*e.g.*, a trademark); (3) the proposed gTLD is contrary to generally accepted legal norms relating to morality and public order; or (4) the proposed gTLD is the subject of substantial opposition from a significant portion of the community to

³² This section provides an overview of the new gTLD application process. ICANN's Draft Applicant Guidebook runs nearly 100 pages and describes the process in much more detail. Potential applicants should closely study this document so they can begin to prepare their applications.

which the string may be explicitly or implicitly targeted. Clearly, the grounds for objection leave much room for interpretation, but ICANN has chosen to remove itself from the process of resolving disputes, opting instead to outsource the process to third-party dispute resolution providers.

If applicants demonstrate the necessary financial and technical resources and survive the objection process, ICANN will review the remaining applications to see if more than one applicant has filed for the same gTLD string. If there is such a conflict, ICANN will either submit the applications to a comparative evaluation or bypass that evaluation and submit the gTLD to an auction among the applicants. Once any gTLD string conflicts have been resolved, ICANN will award the remaining applications with the requested gTLDs, subject to final contract negotiation and technical testing.

Impact

In order to protect their brands, trademark owners will need to closely monitor both the application process and the launch of any approved new gTLDs. First, trademark owners will need to keep watch on the strings that applicants propose for new gTLDs, so as to ensure that no new gTLD will infringe on their trademarks. If an applicant proposes an infringing gTLD, the trademark owner should evaluate whether to file an objection against the application or to allow it to proceed.

Second, once the gTLDs are awarded, trademark owners would be wise to keep abreast of each new gTLD's mechanisms for protecting trademark rights and then to decide whether and how to protect their brands in each gTLD. Some gTLDs are likely to implement pre-launch "sunrise" periods, during which trademark owners are permitted to register their brands as domain names in the new gTLD before the gTLD is opened for general registration. Others are likely to implement "watch lists" that enable trademark owners to monitor domain name applications, but do not confer an actual domain name.

Each new gTLD will likely have its own timeline, rules and procedures for protecting trademarks, and with potentially dozens of new gTLDs, keeping track of each gTLD's policies could present a major challenge for legal departments in companies throughout the world.