Letter From the Chair

By Kimberly A. Paulson, Miller, Canfield, Paddock and Stone PLC
Detroit, Michigan

Greetings Information Technology Law Section Members! It’s unfortunate that my first Letter from the Chair comes at the end of my term, but as you know, there has been some turnover in the newsletter editorial staff. I am happy to say, though, that we have great new editors, and I am excited about the future of our newsletter. I’d like to extend thanks to our outgoing Editor, Matt Jakubowski, for the fine job he has done over the last few years, as well as welcome Brian and Mike.

The timing of the new era of our newsletter coincides with a new era in our Section's history. Of course, last year our Section name was changed to the Information Technology Law Section. We also have a corresponding change in the name of our newsletter. As you can see from the new masthead, it is now the Michigan IT Lawyer. The Section will also soon be sending out the first edition of our new quarterly E-Newsletter, which will keep you updated on upcoming events as well as topics of interest. Look for it in your inbox soon.

The past year has also seen a new emphasis on substantive programming, which will hopefully continue into the future. To that end, we have two exciting programs coming up. At the Section’s Annual Meeting on September 17, we will be hosting a panel of practicing IT lawyers who will speak about “The Practice of Information Technology Law.” The Section is also co-sponsoring a program with ICLE, entitled “Information Technology Law: What Every Lawyer Should Know,” that will be held on October 29. We are very excited about that program, which brings together speakers from all over the country on a variety of IT law topics. More information about both events is provided in this newsletter. Registration has already begun for both; be sure to get your registrations in soon.

The past year also saw a collaboration between our Section and the Litigation Section in the form of a joint newsletter. That project was a terrific success, which benefited the members of both sections. Projects like that bring recognition to the fact that the IT Law field overlaps with so many other practice areas and heightens awareness of our Section and our members. We hope to participate in more cross-section cooperative efforts like that in the future.
Introducing the Co-Editors of *Michigan IT Lawyer*

As the new co-editors of the *Michigan IT Lawyer*, we would like to take this opportunity to introduce ourselves.

**Michael Gallo** is a technical leader for EDS Execuive Support, and has 18 years of experience in various technical and business facets of the information technology industry. Michael has directed numerous deployment, migration, and problem resolution efforts, and has provided leadership for hardware migrations, wireless networking deployments, e-mail migrations, and various application, system, and network upgrades. Michael volunteers with the University of Detroit Jesuit High School and Academy as a member of the board of directors, and as Technology Committee chairperson. Michael has a master of business administration from Marquette University, a master of science in computer and information systems from University of Detroit Mercy, and expects to complete a juris doctorate from the University of Detroit Mercy School of Law in May 2009.

**Brian A. Hall** is an attorney at Traverse Legal, PLC, a law firm dedicated to the global representation of business interests and based in Traverse City, Michigan. Brian’s practice focuses on Internet law, global online brand protection, cybersquatting, domain name disputes, intellectual property, and complex litigation. Brian received a bachelor of science in business/management information systems from Miami University in Oxford, OH and worked as an IT and management consultant with Accenture for two years before attending law school. He received his JD from Michigan State University College of Law, where he also served as executive editor of the *Michigan State Law Review*. While attending law school, Brian served as a law clerk in the civil division of the United States Attorney’s Office—MDFL. Brian is a member of the board of directors of Connectech, Michigan’s premier association for technology professionals. He also enjoys volunteering in various capacities as part of the Rotary Club of Traverse City.

We are both extremely excited to be serving as co-editors of this publication. As you will see, this issue is larger than usual in light of the abundance of material that had yet to be published, including last year’s Edward G. Langs award winning student papers, one of which happens to be by Mr. Gallo. In the future, we fully intend to publish the newsletter at least every quarter in an effort to bring you relevant and timely material. Please do not hesitate to contact us with submissions, feedback, and suggestions. Our goal is to help you become a better Michigan IT lawyer!
In Attempting to Use the Internet to Spread Knowledge and Create Efficient Markets, Is the Google Book Search Project Developed by Google, In Agreement with Existing U.S. Copyright Laws?

By Theo Kountotsis

INTRODUCTION — What is the “Google Book Search Project” that is available on the Internet by Google?

Agreements Entered Into by Google and Third Parties

Google Book Search is an online tool offered by Google that searches the full-text of books (literary works) that Google scans and stores in a digital database. Google first commenced the Google Book Search service in October 2004. The Google Book Search Project relates to two different functions or agreements. One is an agreement between Google and publishers, and the other is an agreement between Google and libraries. The first agreement is based upon an “opt-out” system initialized by Google, where publishers can “opt-out” from the Google Book Search Project at any time after their literary work has been copied and scanned into the Google database. The second agreement allows Google to scan, in certain instances, every literary work that a participating library owns.

Information is Displayed by Google in Three Different Formats

In each case, a user of a computer may access the Google search engine via an Internet connection and pinpoint inquiries by author, title, date of publication, length, subject, and/or keyword of any and all scanned literary works located in the Google database. Three different indexes or views may be displayed on a user's screen after a search has been conducted. These are: (i) a full view, (ii) a limited preview view, and/or (iii) a snippet view. The full view is displayed when a book is out of copyright or the copyright holder has given permission to display the whole book. The limited preview view is displayed when a publisher has agreed to allow users to view predetermined portions of a book. The snippet view allows a user to enter a search term and view up to three different, yet small portions of the book.

At this moment, Google alleges that the Google Book Search Project allows only public-domain works and out-of-copyright material to be downloaded in full.

The Google Book Search Project, as Currently Implemented by Google, is Infringing Copyrights of Authors and/or Publishers Under Current U.S. Copyright Laws

What Works are Protected by U.S. Copyright Laws?

First, in order to establish whether Google is liable under a copyright infringement theory, it is important to determine what types of works U.S. copyright laws protect.

17 U.S.C. §102(a) of the 1976 Copyright Act provides, inter alia, that:

“copyright protection subsists … in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device.”

May 2008 also brought another enjoyable Happy Hour at the Dirty Martini. Members who attend that event always tell me how much they enjoyed the food, drink, atmosphere, and company. We had a large contingency stay for the Second City show this year as well. No one has ever left one of those shows without a smile. For those of you who have never attended one of our Section’s Happy Hour events, I encourage you to give it a try next year. It is always a lot of fun and a great networking event.

Overall, the IT Law Section has had a great year of growth and innovation. Thanks to all the hard-working Council members, our Section is more active and offering more benefits to our members than in years past. I thank all the Council members for their ideas and hard work and all the other Section members who have attended events, written articles, and volunteered to fill positions. Thanks for a great year. I look forward to many more.
In addition, 17 U.S.C. §102(a) states, *inter alia*, that “works of authorship include the following categories: (1) literary works…”

17 U.S.C. §102(b) of the 1976 Copyright Act provides, *inter alia*, that:

“*in no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery …*”

In the instant case, the literary works owned by the authors and/or the publishers are subject to copyright protection because they are original works that are fixed in a tangible medium, thus satisfying 17 U.S.C. §102(a) and 17 U.S.C. §102(b) of the 1976 Copyright Act. Therefore, it is safe to say that the majority of the literary works copied by Google are not ideas in themselves, but expressions of ideas, which are protected by U.S. copyright laws.

What are the Exclusive Rights of an Owner of Valid Copyrighted Works?

Second, in order to establish whether Google is liable under a copyright infringement theory, in addition to determining which works are protected by U.S. copyright laws, it is also important to determine what exclusive rights are provided to an owner of a copyright.

17 U.S.C. §106 of the 1976 Copyright Act states, *inter alia*, that:

“the owner of copyright … has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies or phonorecords; (2) to prepare derivative works based upon the copyrighted work; (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending…”

As a result, the next question is whether Google deprived the copyright owners of any of the above-mentioned exclusive rights. The next section describes the violation by Google of specific exclusive rights provided to authors and/or publishers of valid copyrighted literary works. The rights deemed violated by Google include the right to reproduce and the right to distribute copies of literary works.

**Google Has Violated at Least Two of Exclusive Rights of U.S. Copyright Owners of Literary Works, Namely the Reproduction Right and the Distribution Right, and Google is Therefore Liable for Copyright Infringement**

What are the Elements of Copyright Infringement Under U.S Copyright Laws?

Since literary works are protected under copyright laws (17 U.S.C. §102(a),(b)) and at least two exclusive rights of the authors and/or publishers may have been violated (as described below), a copyright infringement analysis is appropriate. In order to establish whether Google is a copyright infringer, it is necessary to determine what elements are required to prove copyright infringement under U.S. copyright laws.

To begin the analysis, copyright law is a creature of statute and the only rights that exist under copyright law are those granted by statute. Furthermore, there is no scienter requirement in copyright infringement.

17 U.S.C. § 501(b) of the 1976 Copyright Act recites, *inter alia*, that:

“The legal or beneficial owner of an exclusive right under a copyright is entitled ... to institute an action for any infringement of that particular right committed while he or she is the owner of it.”

Therefore, under U.S. copyright law, the authors and/or publishers have a right to institute an action for infringement of their copyrights against Google. However, what elements do courts look to when determining such violation of exclusive rights of owners of valid copyrights? To establish infringement, two elements must be proven:

“(1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original.”
First Element of Copyright Infringement: Ownership of a Valid Copyright on the Literary Works

The first element necessary to prove copyright infringement is ownership and validity of a copyright. How does an author or publisher prove ownership and validity of a copyright? Certificates of copyright registration constitute prima facie evidence of the validity of copyrights and the facts stated in the certificates are prima facie proof of ownership and validity. This merely creates a presumption of validity, meaning that, it is not conclusive on the issue of copyrightability.

In the instant case, it is presumed that the majority of the authors and/or publishers have obtained a certificate of copyright registration for each and every work they possess. Google will most likely not dispute prima facie proof of ownership and validity of the literary works. Thus, the authors and/or publishers may easily prove the first element of copyright infringement.

Second Element of Copyright Infringement: Whether Original Elements of the Literary Works Have Been Copied

The second element necessary to prove copyright infringement is establishing that the literary works contain original elements. How does an author and/or publisher establish that their literary works include original elements? The key to resolving this issue lies in understanding that facts are not copyrightable. The sine qua non of copyright is originality. To qualify for copyright protection, a work must be original to the author.

In Feist, Justice O’Conner declared originality to be an inescapable constitutional requirement for copyright protection for all works of authorship. Original, as the term is used in copyright law, means only that the author independently created the work and that it possesses at least some minimal degree of creativity. The requisite level of creativity is very low and even a slight amount will suffice. Therefore, the standard of originality is low, but it does exist. In other words, there must be something more than a mere trivial variation, something recognizably the artist’s own. The originality requirement mandates that objective facts and ideas are not copyrightable. Similarly, expressions that are standard, stock, or common to a particular subject matter are not protectable under copyright law.

In the instant case, Google is copying all the literary works from certain libraries, whether a copyright exists or not in those literary works. It is apparent that a majority of the literary works contain original elements. Libraries do not carry literary works containing only facts. Thus, the authors and/or publishers may easily prove the second element of copyright infringement.

Consequently, since the authors and/or publishers may easily prove the first and the second elements of copyright infringement, it is necessary to determine which exclusive rights Google has violated. The next section described those rights deemed to be violated by Google. Section B analyzes whether Google has violated the exclusive right to reproduce a literary work and Section C analyzes whether Google has violated the exclusive right to distribute a literary work.

17 U.S.C. §106(1): Who Has the Right to Make Copies In The Instant Case?

17 U.S.C. §106(1) of the 1976 Copyright Act states, inter alia, that:

“the owner of copyright … has the exclusive rights to do and to authorize any of the following: to reproduce the copyrighted work in copies …”

In the instant case, it is undisputed that Google has made unauthorized copies of several copyrighted literary works because Google, admittedly, simply copied each and every literary work in at least one library. Therefore, the authors and/or publishers who own the valid copyrights have the right to reproduce copies of their works, not Google, unless Google had express permission by the valid copyright owners.

Can a library permit a company, such as Google, to scan the library’s entire literary works for the benefit of the company? The answer is “no,” because this is clearly copyright infringement in violation of 17 U.S.C. §106(1). A company, such as Google, does not have a right to copy such literary work without express authorization by the valid copyright owners. Therefore, Google has violated the authors and/or publishers exclusive right to reproduce their copyrighted works.

Continued on next page
Who Has the Right to Distribute Copies of a Literary Work and When is Distribution Permissible by a Buyer of a Copyrighted Literary Work?

17 U.S.C. §106(3): Who Has the Right to Distribute Copies In The Instant Case?

17 U.S.C. §106(3) of the 1976 Copyright Act states, *inter alia*, that:

“the owner of copyright … has the exclusive rights to do and to authorize any of the following: to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending.”36

Therefore, in accordance with 17 U.S.C. §106(3), the valid owner of the copyright has the exclusive right to distribute the literary work. In the instant case, the authors and/or publishers who own the valid copyrights have the right to distribute copies of their works, not Google, unless Google had express permission by the valid copyright owners.

In addition, in the second agreement concerning the partnership libraries, Google scanned all the literary works of a partnership library (e.g., University of Michigan library).37 Google claims to scan only public-domain literary works from other select libraries.38 In addition, each library gets to keep a digital copy of all literary works in its collection that it permitted Google to scan.39 Authorization for Google to scan these literary works is based on permission secured from libraries, not from publishers or authors.40 This approach is clearly not consistent with 17 U.S.C. §106(3).

Can a company, such as Google, create a second electronic copy of the literary works and give such copies, for free, back to the partnership library? The answer is “no” because this is clearly copyright infringement in accordance with 17 U.S.C. §106(3). A company, such as Google, does not have a right to distribute such literary work without express authorization by the valid owner of the copyrighted work. Therefore, Google has violated the authors and/or publishers exclusive right to distribute their copyrighted works.


17 U.S.C. §109(a) of the 1976 Copyright Act states, *inter alia*, that:

“notwithstanding the provisions of §106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.”41

Therefore, in accordance with 17 U.S.C. §109(a), any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy. However, once a copy of the literary work has been distributed and purchased lawfully by a purchaser, the purchaser is entitled to use sell or dispose of the lawful copy in any manner.

17 U.S.C. §109(a) of the 1976 Copyright Act is also referred to as the doctrine of first sale.42 The doctrine of first sale allows the purchaser to transfer (i.e., sell or give away) a particular, lawfully made copy of the protected work without permission once it has been obtained.43 That means the distribution rights of a copyright holder end on that particular copy once the copy is sold.44 The whole point of the first sale doctrine is that once the copyright owner places a copyrighted item in the stream of commerce by selling it, he has exhausted his exclusive statutory right to control its distribution.45

The first sale doctrine is applicable to the instant case. Specifically, Google never obtained a lawful first copy of the literary works that are scanned into its digital database. Instead, in many instances, Google merely copies all the literary works absent any permission from the valid copyright owners. Google never even attempted to purchase a first copy of the literary works. Instead, Google decided to merely “borrow” and copy someone else’s valid copies (i.e., libraries copies). Is a library permitted to allow anyone, whether a corporation or an individual, to copy all its literary works that were lawfully obtained? Does 17 U.S.C. §109(a) of the 1976 Copyright Act state, expressly or implicitly, that the library may “lend” its entire literary works to a corporation, such as Google, for copying?

As a hypothetical, if an individual purchases thousands of literary works and then scans all those works on a personal computer, thus making an electronic copy of every literary work, then may such lawful purchaser use such database to his own benefit? Has the purchaser committed copyright infringement? Does scanning thousands of literary works, whether purchased or not, fall under 17 U.S.C. §109(a), even when such use is not for profit? The answer to such inquiry is “no” because, even
though the purchaser lawfully purchased all the literary works, the purchaser still has no right to make or allow another to make an electronic copy of all those lawfully purchased literary works. This would put 17 U.S.C. §109(a) and 17 U.S.C. §106(1) in direct conflict with each other. The copyright owner does not waive all or any of his exclusive rights because of the first sale doctrine. Therefore, even if an individual purchases a literary work, under 17 U.S.C. §109(a), that individual has “the right to sell or otherwise dispose of the possession of that copy,” which does not include making or allowing others to make additional copies of the literary work. As a result, Google, which is a for-profit company, cannot justify copying entire literary works from libraries, even if Google had permission from such libraries to do so because the libraries, under 17 U.S.C. §109(a), did not have the right to permit copying by others of its lawfully obtained literary works. Therefore, Google has violated the authors and/or publishers exclusive right to distribute their copyrighted works under the first sale doctrine.

Who Has the Right to First Distribution by a New or Novel Means of Distribution to the Public?

The Copyright Act of 1976 is not clear on this issue, and in fact, does not specifically address this issue. The main issue is whether Google has stripped away the control that authors’ and/or publishers’ have in distributing their literary works in a new distribution medium?

In general, when 17 U.S.C. §106(3) is applied to Internet transactions, two questions arise. The first question is whether there is a public distribution. Clearly, posting literary works on a search engine would constitute “public” as the statute requires. The second question is whether the transmission over the Internet falls under “other transfer of ownership” mentioned in §106(3) of the 1976 Copyright Act. Has distribution occurred when a transmission from one computer to several others takes place? The answer should be a resounding “yes” under the “other transfer of ownership.” Does the distribution right extend to works distributed to the public by any type of transmission? When reading the statute in a broad manner, the answer should be “yes.”

Therefore, since the Internet facilitates a public distribution by “other transfer of ownership,” it is clear that the exclusive right to distribute a work by the Internet is a right of the copyright owner under 17 U.S.C. §106(3). However, does this imply that the copyright owner has the right to first distribution in every new medium developed after obtaining an initial copyright? What if a company develops a new technology for distribution and wishes to act as a “middle man”? In other words, in the instant case, Google is acting as a “middle man” between the authors and/or publishers, and the general public. Why should there be such a “middle man” distributor of literary works? Shouldn’t the authors and/or publishers have the right to a first offer of such literary works via a new communication/distribution medium under 17 U.S.C. §106(3)? Who should have the first right to use the Internet as a distribution means for their products? In addition, does allowing Google to act as a “middle man” hurt the authors and/or publishers in economic terms?

Publishers and authors compare Google Book Search to Napster. Napster was conceived as a search engine for music files by using a real-time centralized index of MP3 files contained on users’ computers. Napster was also designed to economize server space, as Google does, by indexing content and linking to it without actually serving it up to Internet users. When several major record labels and owners of music publishing rights sued Napster, Napster sought a safe haven under Sony’s substantial non-infringing use defense. The court in Napster, however, held that Napster was not entitled to the defense because it had actual knowledge that its software was used to infringe music copyrights. The court rejected Napster’s fair use defense based on expert reports showing a decline in sales of music in college markets, as well as a threat to other existing markets.

In addition, the court in Napster found that:

“harm to the market for copyrighted works may include not only harm to an established market, but also harm to the right to develop alternative markets such as legal digital downloads.”

The court in Napster further stated that:

“having digital downloads available for free on Napster necessarily harms the copyright holders’ attempts to charge for the same downloads, and any allegedly positive impact … on plaintiffs’ prior market in no way frees defendant to usurp a further market that directly derives from reproduction of the plaintiffs’ copyrighted works.”

Unlike Napster, Google, via the Google Book Search Project, is not a system that always allows the free downloading of full
copyrighted books or literary works. While Napster enabled users to find copyrighted full-length songs at no charge, Google is not always distributing intact chapters or pages of a literary work still under copyright. In most cases, absent full permission, a preview of a copyrighted literary work will only include bibliographic information with a few sentences of a search term in context.

However, the Google Book Search Project is similar to Napster in that it deprives the authors and/or the publishers the right to develop alternative markets that directly derive from reproduction of the authors and/or publishers copyrighted literary works. Thus, Google may impede authors and/or publishers efforts to develop online markets for e-books.

Finally, concerning the detrimental economic impact the Google Book Search Project may have on authors and/or publishers, one may argue that the Google Book Search Project is unlikely to reduce the sale of printed literary works and that it promises to improve the marketing of literary works via a novel marketing platform featuring short previews. Nevertheless, as the court in Napster stated, and in view of a broad reading of 17 U.S.C. §106(3), the authors and/or publishers should have the first right to distribute their literary works by “other transfer of ownership,” meaning by any new distribution medium later developed or perceived.

CONCLUSION OF SECTION I

Section I of this paper described the Google Book Search Project as currently implemented by Google. It was determined that Google is liable for copyright infringement by establishing (i) what works are protected under U.S. copyright laws and (ii) what are the exclusive rights of an owner of valid copyrighted works. An analysis was performed as to the two elements of copyright infringement, that is, ownership of a valid copyright and copying of constituent elements that are original. It was determined that Google violated at least two exclusive rights, the reproduction right and the distribution right (17 U.S.C. §106(1),(3) of the 1976 Copyright Act).

II - DEFENSES

Since Google may be liable under copyright infringement to authors and/or publishers of valid copyrighted works, as described above in Section I, may Google assert any valid defenses to such copyright infringement charges? It appears that Google has offered two defenses to any copyright infringement allegations that have arisen. The first defense is related to an “opt-out” initiative (not found in the 1976 Copyright Act) and the second defense is related to the fair use doctrine (found at 17 U.S.C. §107 of the 1976 Copyright Act).

DEFENSE 1: Opt-Out initiative: The First Line of Defense That Google Has Offered to Negate Copyright Infringement is an “Opt-Out” Program That Should Not be a Successful Defense Because it Violates Well-Established Principles of U.S. Copyright Law

What is Google’s “Opt-Out” Initiative Offered to Owners of Copyrighted Works?

17 U.S.C. §106 of the 1976 Copyright Act confers on the rights holder of a copyright the exclusive right to control, *inter alia*, reproduction and distribution of a protected literary work. Therefore, in order to use someone else’s copyrighted literary work, one seeks permission from the owner of the valid copyright and negotiates the terms, conditions, and payments for use.

In the first agreement concerning the author and/or publisher rights, Google permits publishers to “opt-out” from the Google Book Search Project at any time. Google claims that for it to actively seek permission from every rights holder in developing a huge digital library of collections would be impractical and prohibitive.

However, how can one announce one’s intention to infringe millions of literary works by making a copy of each work and collectively offer right holders the opportunity not to have their work infringed? This appears to be contrary to 17 U.S.C. §106 of the 1976 Copyright Act. As a result, the authors and/or publishers rightfully claim that Google’s “opt-out” program is contrary to well-established U.S. copyright laws.
Is Google’s “Opt-Out” Initiative Permissible/Legal Under Current U.S. Copyright Laws?

In order to determine if Google's approach via the “opt-out” program is permissible or legal, it is necessary to determine who creates the laws in the U.S. Therefore, the issue is who creates or modifies the laws in the U.S.? Can a corporation, such as Google, modify copyright laws because such laws do not suit Google's needs?

Article I, § 8, clause 18 of the U.S. Constitution states, *inter alia*, that:

“The Congress shall have Power To … make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States …”

Therefore, Congress has the right to make the laws that it deems necessary and proper to carry out its duties. According to the U.S. Constitution, only Congress has such a right, not judges or corporations or any individual. Judges are vested with the power to interpret the law, and as they interpret the law apply it to the facts that they find. Judges must follow the law, as dictated by the statute.

Where a court is asked to state or formulate a common law principle in a new context, there is a general understanding that the law is not so much found or discovered as it is either made or created. Sosa quoted Justice Holmes, stating that:

“in substance the growth of the law is legislative … [because t]he very considerations which judges most rarely mention … are the secret root from which the law draws all the juices of life. I mean, of course, considerations of what is expedient for the community concerned.”

Therefore, the law is a product of the legislative and not the judiciary, and certainly not of a corporation or an individual. It is one thing to request a judge to stretch or expand a law, and one thing to request and self-adhere to a total reversal of a law, as Google proposes in the instant case.

17 U.S.C. § 106 of the 1976 Copyright Act specifically states, *inter alia*, that:

“the owner of the copyright has the exclusive right to: (1) to reproduce the copyrighted work in copies or phonorecords … (3) to distribute copies or phonorecords of the copyrighted work to the public …”

Clearly, 17 U.S.C. § 106 implies that one must seek permission from the copyright owner to use a work owned by the copyright owner. Clearly, the burden seems to be placed on Google in the instant case. This burden cannot be shifted, not in accordance with present U.S. copyright laws, to the copyright holders, unless Congress amends this portion of the copyright statute. Google's strategy to reach out directly to authors and/or publishers is similar to the attempts of Napster to bolster their fair use and substantial non-infringing use defenses by inviting musicians and unsigned bands to authorize the free downloading of their work from these services. However, this strategy was not successful for Napster, and should not be successful for Google. Therefore, Google's first defense should fail. However, Google can assert a second line of defense.


Can Google Rely on Kelly to Convince a Court That it is Fair Use to Utilize Literary Works in Such a Manner Anticipated by Google? What is the Difference Between the Kelly Decision and Google?

Once again, a party is asking the courts of the U.S. to extend and/or expand the fair use doctrine of the 1976 Copyright Act. A claim of copyright infringement is subject to certain statutory exceptions, including the fair use exception. This exception permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster.

17 U.S.C. § 107 of the 1976 Copyright Act states the four statutory factors considered in making the fair use determination, which are, *inter alia*:

“ (1) the purpose and character of the use …; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.”
Kelly is a professional photographer who has posted several photographs he has taken on his website.\textsuperscript{70} Arriba Soft operates an Internet search engine that displays its results in the form of small pictures rather than the usual form of text.\textsuperscript{73} Arriba Soft builds its database of small pictures, called thumbnails, by copying full-size images from other websites.\textsuperscript{72} However, the copies generated are smaller than the original images copied and they are of a lower resolution.\textsuperscript{73} Once the thumbnails are created by Arriba Soft's software, the original full-size image is removed from its database.\textsuperscript{74} In Kelly, the court found that Arriba Soft's search engine was a transformative use sufficient enough to be a fair use.\textsuperscript{75} Indexing information alone may not be copyright infringement. Therefore, displaying limited quotes from a literary work may also be consistent with fair use. However, that may depend on the specific quote extracted from the literary work.

A major distinction between Kelly and Google is that in Kelly, the content owners voluntarily uploaded the images onto the Internet. In contrast, Google is copying material to a new, distinct database to enable a search capability.\textsuperscript{76} In addition, Arriba Soft never kept a copy of any of the images. In contrast, Google is making and keeping copies in its database.\textsuperscript{77} In fact, Google is further proving the libraries with an electronic copy of each literary work it has copied.\textsuperscript{78}

A similarity between Arriba Soft and Google is that Arriba Soft is directing all users to the original website(s) where the images may be found and purchased directly from the copyright owner. Google appears to be performing this same task. In other words, if Internet users are interested in purchasing a literary work, Google links such users to the authors and/or publishers websites for purchasing purposes. Nevertheless, it appears that the court in Kelly may have misapplied the law and could be overruled by the Supreme Court in a potential Google ruling.

Specifically, 17 U.S.C. § 106 of the 1976 Copyright Act specifically states, \textit{inter alia}, that:

\begin{quote}
“the owner of the copyright has the exclusive right to: distribute copies … to the public by sale or other transfer of ownership, or by rental, lease, or lending; and in the case of literary … works … to display the copyrighted work publicly.”\textsuperscript{79}
\end{quote}

Therefore, Kelly has the right to distribute and display the work according to 17 U.S.C. § 106. Even if the fourth factor of the fair use doctrine, namely, the effect on the potential market tilts toward Arriba Soft, according to a strict reading of § 106 of the Copyright Act, it is the author who should have the first opportunity to distribute and display his works in any means he or she sees fit. Therefore, it appears that the Kelly court may have misapplied U.S. copyright laws, and specifically, the right to first distribute and the right to first display a literary work. Is there a strong possibility that the U.S. Supreme Court will overrule Kelly in deciding the two pending lawsuits against Google,\textsuperscript{80} assuming the two pending cases reach the U.S. Supreme Court? That could be very likely in order to restore order in U.S. copyright laws and their application.

In the instant case, it does not appear the Google can successfully rely on the Kelly decision because (i) there are significant factual differences between Kelly and Google, and (ii) Kelly may be a decision that would be overruled by the U.S. Supreme Court, due to misapplication of U.S. copyright laws. Thus, the second line of defense, namely the fair use doctrine should also fail.

\textbf{Can Google Rely on Sony to Convince a Court That it is Fair Use to Use Literary Works in Such a Manner Anticipated? What is the Difference Between the Sony Decision and Google?}

In Sony, movie studios sued Sony, the manufacturer of the Betamax videocassette recorder, and the Supreme Court refused to find Sony liable for the allegedly infringing conduct of Betamax users, noting that a finding of contributory infringement is normally the functional equivalent of including an article of commerce within Sony's copyright monopoly.\textsuperscript{81} The Court held that the sale of the Betamax or any other articles of commerce capable of copying protected works is not a form of contributory copyright infringement if the product is widely used for legitimate, unobjectionable purposes or is capable of substantial non-infringing uses.\textsuperscript{82} In Sony's case, a non-infringing use of the Betamax was taping television programs to watch at a later time, or “time-shifting,” which was fair use because there was little evidence that television ratings or advertising revenues would decrease, or that motion picture attendance or videotape rentals would decrease as television taping of motion pictures became an alternative.\textsuperscript{83}

In particular, the Court in Sony stated, \textit{inter alia}, that:

\begin{quote}
“(1) there is a significant likelihood that substantial numbers of copyright holders who license their works for broadcast on … television would not object to having their broadcast \textit{time-shifted} by private viewers (i.e., recorded at a time
when the VTR owner cannot view the broadcast so that it can be watched at a later time); and (2) that there is no likelihood that time-shifting would cause non-minimal harm to the potential market for ... respondents’ copyrighted works.”

In addition, the Court stated that:

“The VTR’s are therefore capable of substantial non-infringing uses. Private, non-commercial time-shifting in the home satisfies this standard of non-infringing uses.”

Therefore, the Court noted, there was evidence that time shifting would aid Sony rather than harm them by expanding their audiences to include people away from home during the time of initial broadcast of a program. The Court stated that Universal City Studios had not come forward with evidence of any likelihood of non-minimal harm to the potential market for, or the value of, their copyrighted works that would throw the fair use status of time shifting into doubt.

In the instant case, can Google claim that an infringing activity that facilitates an arguably legitimate use is indeed a fair use in accordance with Sony? Is Google’s digital scanning only incidental to the useful function of indexing?

The major difference between Sony and Google is that Sony dealt with a product, the product in itself, which was only capable of copying protected works. Sony did not copy every copyrighted movie in existence and then offer a snippet of a movie to each user of a VTR. In other words, in Sony, the product itself is associated with the infringement. In contrast, the Google Book Search Project, as currently implemented, requires Google to copy all works in a separate digital database, and then offer access to such database. In other words, the product in itself, the search engine or searching software, is not a product in itself capable of infringement. The copyright infringement occurred by Google staff before incorporated into the product, the product being the Google search engine.

Thus, in the instant case, it does not appear the Google can successfully rely on the Sony decision because (i) there are significant factual differences between Sony and Google, and (ii) Sony’s legal precedent does not appear to be relevant or controlling in the instant case. Therefore, reliance on the Sony case should not benefit Google’s arguments.

CONCLUSION OF SECTION II

Section II of this paper described the defenses that Google may potentially assert to defend itself against potential copyright infringement activities. It was determined that Google may assert two defenses. The first defense relates to an “opt-out” initiative that finds no support in the 1976 Copyright Act, and is evidently a product of Google’s attempt to redefine copyright laws. The second defense relates to the fair use doctrine, which finds support in existing U.S. copyright laws (17 U.S.C. § 107). Two relevant cases that Google can rely on to determine the effectiveness of the fair use doctrine were discussed. These cases were: Kelly v. Arriba Soft and Sony v. Universal City Studios. The determination is that Google will not be able to rely on either the first defense (Kelly) or the second defense (Sony) to successfully fight off copyright infringement allegations.

III - ADDITIONAL ISSUES WITH THE GOOGLE BOOK SEARCH PROJECT

The Concept of the Google Book Search Project Providing a User a Snippet of Information Regarding a Literary Work May Not Survive the Harper & Row Test Because Authors and/or Publishers May Possess Such Exclusive Right Under Existing U.S. Copyright Laws

Is a Snippet of Information Considered a Fair Use In Every Circumstance?

Google may allow users who sign in to browse up to two pages before and after a search result, with additional limits on multiple searches or pages previewed per book. Google logs its users’ page views to enforce aggregate browsing limits, so users’ must obtain a Google account and sign in, thus enabling Google to track the pages they have viewed. Users are not allowed to copy, save or print from their Internet browser. However, as the next case illustrates, allowing users to browse up to two pages of material from a literary work may cause a serious copyright infringement issue.

In Harper & Row, the former President Gerald R. Ford contracted with Harper & Row to publish his unwritten memoirs, which were to contain his thoughts on the Watergate crisis and his pardon of President Nixon. Harper & Row had acquired the right to publish the memoirs in book form and had a licensing agreement with Time Magazine for Time Magazine to use
minor, predetermined, pre-publication excerpts to promote the book.92 However, before Time Magazine obtained an authorized excerpt, Nation Enterprises stole the manuscript from Harper & Row, and published the relevant excerpts.93 The article written and published by Nation Enterprises was 2,250 words long, and approximately 300 of those words were subject to copyright protection because they were verbatim quotations from the memoirs.94

The Supreme Court, in *Harper & Row*, held that Nation Enterprises use of these verbatim excerpts from the unpublished manuscript was not a fair use.95 Therefore, even though only 300 words were subject to copyright infringement, a small excerpt containing those 300 words was enough not to be fair use under the fair use doctrine of 17 U.S.C. § 107 of the 1976 Copyright Act.

In the instant case, when an Internet user accesses the Google Book Search Project, the user is permitted to run three searches, each with a separate key term.96 Google does not make an attempt to distinguish between facts and original elements when a search is conducted.97 Thus, an Internet user using the Google Book Search project may be able to access original excerpts that are copyrighted, thus violating U.S. copyright laws. Consequently, a snippet of information is not considered a fair use in any and all cases, as illustrated in *Harper & Row*. Since Google has not offered a function that denies users specific snippets from the literary works, there is a high probability that a user may access copyrighted works in violation of the law.

**What if the Excerpts Taken by an Internet User Are Mostly the Expression of an Idea Instead of Merely Ideas or Facts?**

In *Harper & Row*, the Court stated, *inter alia*, that:

“… it is true that no author may copyright facts or ideas. The copyright is limited to those aspects of the work termed as “expression” that display the stamp of the author’s originality.”

In the instant case, Google does not, and probably cannot, distinguish between what is “original expression” and what is “fact” in a literary work. In order to do so, Google would probably have to actually read every literary work that Google is copying. That may be an impossible task. However, it can be assumed that a library having at least 1 million literary works contains several thousands of literary works that can be described to contain expression that constitutes originality. Therefore, if Google cannot discriminate between “facts” and “original expression” in such literary works, how can Google guarantee that users will not simply search and read mostly or only original expressions of authors or the heart of a literary work? It appears that the Google Book Search Project has the potential to violate the holding in *Harper & Row* if Google cannot provide for the capability of distinguishing between excerpts containing ideas and expressions of ideas. Therefore, Google would be found liable under copyright infringement.

**What if the Excerpts the Internet User Retrieves Are the Heart of the Book?**

In *Harper & Row*, the Court further stated, *inter alia*, that:

“… Nation Enterprises took what was essentially the heart of the book. A Time Magazine editor described the chapters on the pardon as the most interesting and moving parts of the entire manuscript. According to *Harper & Row*, a taking may not be excused merely because it is insubstantial with respect to the infringing work. As Judge Learned Hand cogently remarked, no plagiarist can excuse the wrong by showing how much of his work he did not pirate.”

Can Google assert that this taking was merely insubstantial, even though the small excerpts it provides to Internet users is insubstantial? What if the excerpt provided by Google contains the heart of the literary work? It appears that the Google Book Search Project has the potential to violate the holding in *Harper & Row* if Google allows users to access the heart of every book. Since Google does not provide a function that clearly distinguishes between “facts” or “ideas” and “expression of ideas,” Google would be violating U.S. copyright laws.

**Who Has the Right to Decide Which Portions of a Literary Work May be Presented to Potential Purchasers of the Literary Work?**

In *Harper & Row*, the Court also stated, *inter alia*, that:

“ Fair use was traditionally defined as a privilege in others than the owner of the copyright to use the copyrighted material in a reasonable manner without his consent. The author’s consent to a reasonable use of his copyrighted works had always been implied by the courts as a necessary incident of the constitutional policy of promoting the progress of sci-
ence and the useful arts, since a prohibition of such use would inhibit subsequent writers from attempting to improve upon prior works and thus ... frustrate the very ends sought to be attained.”100

In the instant case, Google does not afford or even permit the authors and/or publishers with the opportunity to decide which portion(s) of their copyrighted work(s) may be presented to Internet users searching literary works via the Google Book Search Project. According to Harper & Row, the owners of the copyrights have at least a saying into which portion(s) are provided to the general public free of charge.101 In fact, the owners of the copyrighted works seem to be entitled to a reasonable consent to which portion(s) of their literary works are to be utilized.102 Clearly, in accordance with Harper & Row, the decision of permissible portion(s) of literary works should be the choice of owners of copyrighted works only, not the choice of Google or various random users utilizing the Google Book Search Project.

In Harper & Row, the Court additionally stated, inter alia, that:

“Placed in a broader perspective, a fair use doctrine that permits extensive prepublication quotations from an unreleased manuscript without the copyright owner’s consent poses substantial potential for damage to the marketability of first serialization rights in general. Isolated instances of minor infringements, when multiplied many times, become in the aggregate a major inroad on copyright that must be prevented.”103

Therefore, Google could be held liable for copyright infringement even if Google only provides a “snippet” of information. One may argue that digital sampling permits consumers to explore literary genres and excerpts before they buy, avoiding many inefficient purchases based on inadequate or misleading information.104 This may true, however, Google is still required to protect the rights owned by copyright owners. That copyright is intended to increase and not to impede the harvest of knowledge.105 However, the rights conferred by copyright are designed to assure contributors to the store of knowledge a fair return for their labors.106 Thus, there needs to be a balancing act between the right of the owners and the right of the public to acquire knowledge. It appears that Google has mistakenly tilted this balance in its favor and should be held liable for copyright infringement.

CONCLUSION OF SECTION III

Section III of this paper described additional issues that may arise because of the implementation of the Google Book Search Project. It was determined that the Google Book Search Project may not survive the Harper & Row decision. Even though Google provides a snippet of information to the Internet user, such snippet of information has no restrictions that limit the type of information that an Internet user may access. As a result, if a user retrieves the heart of a book, Google may be liable for copyright infringement. In addition, it was determined who has the right to decide which portions of a literary work may be presented to potential purchasers of the literary work. Once again, the authors and/or publishers of the copyrighted works have the right to decide such matters, not Google or random Internet users utilizing Google Book Search.

IV - WILL THE GOOGLE BOOK SEARCH PROJECT REQUIRE A COPYRIGHT REFORM BY CONGRESS?


Would it be absurd, inconvenient or inefficient to require a search engine, such as Google, to get individualized permission from every author and/or publisher to create a card catalogue? Indeed, such a task would be extremely burdensome if not impossible for a search engine. However, under current U.S. copyright laws, this appears to be required. Can U.S. copyright laws be amended to provide for a “Google exception”? In order to answer this question, it is necessary to look into what are the constitutional purposes and limitations of U.S. copyright law.

The Constitutional Purpose of the 1976 Copyright Act is to Promote the Progress of Science and the Useful Arts by Balancing the Need to Provide Authors with a Special Reward and With the Need to Provide the Public Access to New Knowledge

Article I, § 8, clause 8 of the U.S. Constitution states that:

“Congress shall have Power ... To promote the Progress of Science and useful Arts, by securing for limited Times to Au-
thors … the exclusive Right to their respective Writings and Discoveries.”107

This limited grant is a means by which an important public purpose may be achieved.108 It is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired.109 This clause seems to suggest that the dominant purpose of the Framers was to promote the creation of knowledge, so as to enhance public welfare. This goal is to be achieved through provisions of an economic incentive, that being, a monopoly of a limited time to authors of creative works. Therefore, how can Google achieve a balance between the owners of the copyrighted works and the need to provide the public with access to knowledge?

Proposed Legislation That Can Accommodate the Competing Needs of Content Providers and Content Users on the Internet May be in the Form of Reducing Holdout Power of Copyright Owners and Pre-empting the CTEA With Assistance of an International Treaty

What proposed legislation can accommodate the competing needs of content providers and content users on the Internet? What recommended copyright reform may be necessary to aid Google in achieving its Google Book Search Project and be consistent with the U.S. Constitution?

Reducing the Holdout Power of Valid Copyright Owners

17 U.S.C. § 302 of the 1976 Copyright Act states, inter alia, that:

“Copyright in a work created on or after January 1, 1978, subsists from its creation and … endures for a term consisting of the life of the author and 70 years after the author’s death.”110

In Eldred, the Supreme Court upheld the constitutionality of the Copyright Term Extension Act (CTEA) of 1998.111 However, this holding appears to have adopted a policy of perpetual copyrights, under which most of the 20th century copyrights will last until the next century.112 A copyright of a century or more creates a virtually perpetual copyright and leaves the public with almost no expectation of a usable public domain.113 Under the regime of near perpetual copyright, a vast array of political, cultural, and economic history will remain unavailable to the public in a meaningful way for many more years.114

Therefore, even though the Court in Eldred stated that the CTEA is constitutional, in reality the length and breadth of copyright duration negatively affects the establishment of a digital library and negatively affects Google’s Book Search Project. The scanning of books and images is arguably an invasion of a copyright owner’s rights. However, what can be done by Congress to allow Google to continue its initiative and simultaneously reward authors for their contributions?

Can the CTEA be Pre-empted by an International Treaty?

The CTEA extended copyright terms in the U.S. by 20 years.115 § 302 of the original Copyright Act of 1976, effective January 1, 1978, permitted a term of life of the author plus 50 years for an individual author. However, due to the CTEA, § 302, as of 1998, has been amended to protect copyright works for a term of life of the author plus 70 years for an individual work. The CTEA also affected copyright terms of copyrighted works published prior to January 1, 1978.116 Therefore, under the CTEA, no works made from 1923 until 1998, that were still copyrighted in 1998 will enter the public domain until 2019 unless the owner of the copyright releases them to the public domain.117

However, there is a possibility for Congress to amend the 1976 Copyright Act and nullify the Eldred decision by the U.S. Supreme Court. Congress may find support in an international treaty, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights or TRIPS agreement, of which the U.S. is a member since January 1, 1995.118

Specifically, Article 12 of the TRIPS agreement states, inter alia, that:

“Whenever the term of protection of a work … is calculated on a basis other than the life of a natural person, such term shall be no less than 50 years from the end of the calendar year of authorized publication, or, failing such authorized publication within 50 years from the making of the work, 50 years from the end of the calendar year of making.”119

Therefore, the TRIPS agreement provides for a minimum of 50 years, if the copyright term is calculated on a basis other
than the life of a natural person. In order for the U.S. to be compliant with the TRIPS agreement, Congress can amend the U.S. copyright laws, and in particular, § 302 to state that the duration of U.S. copyright laws are 50 years from publication, without having a relationship between the duration of the copyright and an author's death. This solution does not entirely solve the Google Book Search Project issues, however, it does assist Google and sets forth a course in the right direction concerning compatibility of U.S. copyright laws and Internet laws.

CONCLUSION OF SECTION IV

Section IV of this paper described other legal avenues that Google may possess to successfully implement the Google Book Search Project. The constitutional purposes and limitations of U.S. copyright law were analyzed and it was determined that proposed legislation that can accommodate the competing needs of content providers and content users on the Internet may be in the form of reducing holdout power of copyright owners and pre-empting the CTEA with assistance of an international treaty, such as TRIPS.

V - OVERALL CONCLUSION

In the Copyright Act of 1976, Congress sought to benefit the public by encouraging an artist's creative expression. Congress drew the boundaries of copyright protection to achieve this goal. Congress granted artists the exclusive right to original works, thereby giving them financial incentive to create works to enrich society. Nevertheless, Congress denied artists exclusive rights to ideas and standard elements in their works, thereby preventing them from monopolizing what rightfully belongs to the public. According to this understanding, the focus of American copyright law is primarily on the benefits derived from the public from the labors of authors and only secondarily on the desirability of providing a reward to the author in recognition of his creative accomplishment. Therefore, copyright is seen as a means by which the general welfare is advanced through the provision of economic incentives to creators of new works of the intellect.

However, it was determined that Google is liable for copyright infringement. An analysis was performed as to the two elements of copyright infringement, that is, ownership of a valid copyright and copying of constituent elements that are original. It was also determined that Google violated at least two exclusive rights (i.e., the reproduction right and the distribution right). It was further determined that Google may assert two defenses. The first defense relates to an “opt-out” initiative that finds no support in the 1976 Copyright Act. The second defense relates to the fair use doctrine, which finds support in existing U.S. copyright laws (i.e., 17 U.S.C. § 107). Two relevant cases that Google can rely on to determine the effectiveness of the fair use doctrine were discussed (i.e., Kelly v. Arriba Soft and Sony v. Universal City Studios). However, the determination is that Google will not be able to rely on either of these cases to successfully fight off copyright infringement allegations. In addition, it was determined that the Google Book Search Project may also not survive the Harper & Row decision. Even though Google provides a snippet of information to the Internet user, such snippet of information has no restrictions that limit the type of information that an Internet user may access. As a result, if a user retrieves the heart of a book, Google may be liable for copyright infringement.

The constitutional purposes and limitations of U.S. copyright law were analyzed and it was determined that proposed legislation that can accommodate the competing needs of content providers and content users on the Internet may be in the form of reducing holdout power of copyright owners and pre-empting the Copyright Term Extension Act (CTEA) with assistance of an international treaty, such as Trade-Related Aspects of Intellectual Property Rights (TRIPS).

As a result, the Google Book Search Project appears to be doomed without copyright law reform initiated by Congress.

In conclusion, Google's copyright infringement litigation is not only about Google. Google's use of the Internet as a distribution means for vast amounts of information directly challenges copyright laws around the world. Eventually, the Google decisions will help determine whether U.S. copyright laws are compatible with U.S. Internet laws, and if not, how will the courts and/or Congress make the two fields of law compatible. This promises to be quite a challenge.

ENDNOTES

2 Id.
4 Id.
6 Id.
8 Id.
9 Id.
10 Id.
11 Id.
12 Id.
13 Id.
15 Id. (emphasis added).
20 Benchmark Homes, Inc. v. Legacy Home Builders, L.L.C., 2006 WL 208830, 3 (7th Cir. 2006).
23 Id.
24 Feist Publ’s, Inc., 499 U.S. at 345.
25 Id.
26 Id.
27 Id. at 346.
28 Id. at 362.
29 Id. at 345.
30 Id.
31 Satava v. Lowry, 323 F.3d 805, 810 (9th Cir. 2003).
32 Id.
33 Id.
34 Sony Corp. of America, 464 U.S. at 461-62 (emphasis added).
35 Google Book Search, supra note 7.
36 Sony Corp. of America, 464 U.S. at 461-62.
37 Google Book Search, supra note 5.
38 Id.
39 Google Book Search, supra note 7.
40 Id.
43 Id.
44 Id.
45 Quality King Distributors, Inc., 523 U.S. at 152.
48 Id. at 1011-12.
49 Id. at 1020.
50 Id.
51 Id. at 1016.
52 Id. at 1017 (emphasis added).
53 Id.
54 Google Book Search, supra note 7.
55 Napster, 239 F.3d at 1011.
56 Google Book Search, supra note 7.
57 Id.
59 Google Book Search, supra note 5.
65 Id. (emphasis added).
67 Kelly v. Arriba Soft Corp., 280 F.3d 934, 940 (9th Cir.
2002).

Dr. Seuss Enterprises, L.P. v. Penguin Books USA, Inc., 109 F.3d 1394, 1399 (9th Cir. 1997).


Kelly, 280 F.3d at 938.

Id.

Id.

Id.

Id.

Id.

Google Book Search, supra note 7.

Id.

Id.


Sony Corp. of America, 464 U.S. at 441.

Id. at 442.

Id. (emphasis added).

Id. (emphasis added).

Id. at 453.


Id.

Id.


Id.

Id.

Id.

Id.

Google Book Search, supra note 7.

Id.


Id. at 549.

Id.

Id.

Id.

Id. at 569.

See Travis, supra note 58, at 89.


Id. at 546.

Eldred, 537 U.S. at 223 (emphasis added).

Sony Corp. of America, 464 U.S. at 429.

Id.

Eldred, 537 U.S. at 195-96 (emphasis added).

Id. at 218.


Id. at 793.

Id.


Id. at 203-04.

Id.

VoIP—A Technology Coming of Age

By Michael Gallo, University of Detroit Mercy School of Law

Introduction

The first telephone call using “Voice over Internet Protocol” (VoIP) was made in 1995.1 Despite the novelty of making a “telephone” call through a computer and avoiding long distance charges, “quality was low due to choppy sound, echoing, and missed data packets that had been accidentally routed to unknown locations.”2

VoIP is an Internet application that allows voice communications in real time.3 After a decade of limited use, VoIP is on the cusp of becoming an essential medium of voice communication, based on economic advantages the technology has over traditional telephone services.4 While VoIP appeals to consumers seeking to lower monthly bills,5 businesses are attracted by the ability to integrate voice and e-mail communications with the capability to locate individuals, while generating cost savings and increasing operational efficiency.6 VoIP allows telecommunications providers to leverage wired networks to support both voice and data services, and supports the federal government’s goal of expanding broadband services nationwide.7

This comment compares VoIP to traditional telephone services by reviewing the technologies, federal policies, regulatory findings, and administrative rulings that have enabled the tremendous growth of VoIP to date. The comment then looks at the VoIP security policies of 911 system availability to public emergency services, and law enforcement access to VoIP communications.

POTS versus VoIP – Definitions and Technology Differences

Traditional telephone service, known as “Plain Old Telephone Service” (POTS), uses a direct, continuous connection that a local telephone company’s Public Switched Telephone Network (PSTN) controls using circuit-switching technology.8 For the duration of a traditional telephone call, the PSTN dedicates a logical connection between the calling parties.9

POTS is extensively regulated and is classified by the Telecommunications Act of 1996 (the Act) as “telecommunications,”10 which is “the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information as sent and received.”11 The PSTN is also extensively regulated by the Act but is classified as “telecommunication services,”12 which is defined as “the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.”13

In addition to the basic services of “telecommunications” and “telecommunication services,” Congress defined the enhanced service of “information services,” and the Federal Communications Commission (FCC) was tasked with aligning various technologies into these classifications and their respective regulatory challenges.14

Internet telephony, such as VoIP, allows a caller to make at least a portion of a telephone call through an Internet connection instead of a standard telephone line.15 Functionality varies, as some providers require calls be placed only to accounts serviced by that provider, while other providers support calls to any tele-
phone number. Some providers require use of a computer or a dedicated VoIP telephone, while others enable use of a standard telephone and the PSTN through a special adaptor.

Internet Protocol (IP)-enabled “services work much like traditional data transmission: voice sounds are broken down into binary code, distributed across data networks, and reassembled at the receiver’s location.” Many VoIP services make use of a “Session Initiation Protocol” (SIP) which performs the tasks associated with initiation and termination of a call, allowing the call to be transmitted completely over the Internet, or routed to an Internet gateway connecting to POTS.

Traditional telephone services transmit calls using ‘circuit switching,’ in which a line (a circuit) is opened and maintained for exclusive use by the caller. On the other hand, VoIP services transmit calls using a more efficient process of ‘packet switching,’ in which a line is used only while packets of data are transmitted. In packet switching, call activity is divided into individually addressed packets that are sent over a network, and the packets are then reassembled at the destination address. When compared to circuit switching, packet switching reduces transmission cost, frees circuits for other uses, and allows computers to send and receive multiple transmissions at a time. Eventually, packet switching is expected to replace circuit switching for all telephony services.

Congress defined “information service” as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.”

Congress has yet to provide a legal definition for VoIP. As the FCC has determined that Congress intended “telecommunications service” as a basic service, and “information service” as an enhanced service, VoIP’s service classification “depends upon whether or not it more closely resembles the basic/telecommunications service or enhanced/information service definitions as laid down by Congress and the FCC.”

POTS versus VoIP – Death or Convergence?

“The Internet is going to swallow telecommunications. Data traffic is growing much faster than voice, and promises to dominate future capacity demands on all major networks…. There is no doubt which way the wind is blowing.”

VoIP Advantages and Disadvantages

VoIP has several significant advantages over traditional telephone services, including cost. VoIP service rates for a consumer typically range from $10 to $40 per month, including unlimited local and domestic long-distance calls, while traditional telephone services cost about $50 per month and may not include long-distance charges, taxes, or fees. Another significant VoIP advantage is portability, in that traditional services tie the customer’s telephone number to a physical location, while VoIP enables a customer to make calls from any Internet connection in the world.

VoIP also has potential disadvantages. Though the quality gap is narrowing, VoIP “service is not as reliable as traditional telephone service provided by incumbent phone companies.” Another concern is that VoIP requires both an Internet connection and electrical power to place a call, while wireline telephone service provides “enough power to operate a customer’s phone through his or her phone line.” In other words, in a power outage, a VoIP call cannot be placed, which could be “disastrous in an emergency,” and loss of telephone services during an outage could significantly disrupt the business environment. A third concern is that denial of service attacks, in which a malicious person floods the network with packets that disrupt service, are more likely and more disruptive in an IP based network than such attacks are in the PSTN. A fourth concern regards the relative ease and low cost of VoIP “spoofing,” where misrepresentations by the caller can pose a significant economic threat to businesses.

Reliability of the PSTN is taken for granted, but “VoIP could change both the perception and the reality of ever-present telephone service because it suffers the same vulnerabilities to malicious electronic attack as other digital networking technologies.” Hackers and Internet viruses, which have been an insignificant threat on the PSTN, pose significant risk of “cascading disruptions due to interconnection of networked systems.” “An attack on any of the approximately 96,000 networks interconnected as the Internet could cripple that infrastructure, and with the size of the Internet doubling approximately every 24 months, the potential for attack grows.”
VoIP’s Converging Service Models

There are several VoIP service models, many of which converge with traditional telephone services. In the “telephone-to-telephone” model, the caller dials from any telephone into a provider’s gateway, which connects the caller through the provider’s Internet network. In the “telephone-to-computer” model, the caller dials a special number to connect to a recipient’s computer that includes VoIP software. A “computer-to-telephone” call reverses the process, with the caller’s computer connecting to the recipient’s telephone, and with the call generating per-minute service charges comparable to “telephone-to-computer” service charges. In any of the above models includes a traditional telephone and telephone number, Internet access between the traditional telephone system and the network connection can be provided by a traditional telephone service provider, a VoIP service provider, or a third-party Internet Service Provider (ISP).

In the “computer-to-computer” model, a vendor such as Pulver.com or Skype might provide VoIP services that “focus their core service on facilitating voice communications between computer users on the Internet, without necessarily connecting to the traditional phone system.” Skype is a popular VoIP application that enables free computer-to-computer calling, while Pulver.com’s “Free World Dialup” service can be used through “a variety of connection devices, from softphones to hardware IP telephones.” Some believe that a pair of computers, each configured with a microphone, speakers, sound card, an Internet connection, and VoIP software, is the simplest way to set up a VoIP service that enables calls that “are free regardless of the distance.”

The convergence of communication platforms, the array of possibilities in end-to-end networks, and the variety of technologies among service providers challenges the current telecommunications regulatory model. Though forcing new communication offerings to fit old assumptions and definitions may be easier than creating a new regulatory model, existing regulations are often over-inclusive or under-inclusive, and fail to “address unique qualities that the technology may possess.” “Thus, the need for new leadership by the [Federal Communications] Commission as expert agency becomes increasingly clear,” and “only by discarding these outdated analogies and clearly and proactively enunciating the right boundaries for state and federal action will the Commissioners find their way to a new regulatory system that intelligently protects consumer interests, encourages investment, and recognizes the unique and essential characteristics of individual services and technologies.”

POTS versus VoIP—Policy Challenges

The Communications Act of 1934 separated telephone regulation by intrastate and interstate services. Congress passed the Federal Telecommunications Act of 1996 “in an attempt to end the judicial micromanagement of the telecommunications industry,” and to create a policy framework that enabled competition in order to promote the development of advanced telecommunication and information technology.

Classification Determines VoIP Regulation

The Telecommunications Act provides a framework of regulation by “pigeonhole,” in which each classification includes technology specific business models and applications, and each classification has a unique “regulatory scheme and set of institutional arrangements.” The classification assigned to each service identifies rights and responsibilities of the service provider, the provider’s competitors, consumers, and various government entities, but classifications have caused much uncertainty regarding VoIP regulation, because many of the differences that distinguish between information services and telecommunication services have disappeared.

While regulation by classification was relatively simple when networks were based solely on analog technology, IP technologies threaten to make everything “data,” which challenges a framework that presumed each service could be assigned to a specific category, and that “each service had discrete physical plant and outputs.” Whether VoIP is determined to be a telecommunication service or information service is important, because although the Telecommunications Act allows state regulation of telecommunication services, the Act preempts states from regulating information services. The FCC’s policy of not regulating information services “preserves the Internet as a free and open platform for innovation,” and “removes barriers to investment and deployment of Internet applications and services by ensuring that Internet applications remain insulated from unnecessary and harmful economic regulation at both the federal and state levels.”

In other words, determination of VoIP service type determines VoIP policy, but before putting the “VoIP service type” cart
before the “VoIP policy” horse, a look at the process of setting policy may be appropriate.

Policies, Not Classifications, Should Determine VoIP Regulation

Policy setting resolves around three questions: 1) what are the objectives, goals, and concerns; 2) what approach should be used to implement the policy; and 3) do the results satisfy the objectives, goals, and concerns.64

“In terms of communications policy, classical policy concerns addressed market power.”65 When the Telecommunications Act passed, services were offered by telecommunication monopolies that could “engage in anticompetitive behavior,”66 while information service providers lacked market power and were dependent upon the physical network services of telecommunication monopolies.67 For that reason, the FCC regulated telecommunication services for the protection and benefit of information service providers.68

To implement Congress’ communications policies thorough regulations, the FCC separated “basic services” from “enhanced services,” and both service types were defined using a functional approach.69 The FCC determined “the classification of a service under the 1996 Act depends on the functional nature of the end-user offering.”70

Recently, a “layered model” approach has been advanced as a theoretical alternative to the functional model approach, to better classify services into areas of policy concern.71 The layered model separates services (and thereby policies) by “1) physical network, 2) logical or computer networks, 3) applications, and 4) content.”72 Though few jurisdictions fully apply the layered model, several states distinguish between the physical network and voice applications, allowing placement of voice applications as a service belonging to an unregulated, competitive market.73 The layered model brings focus on network architecture, interconnection, and functional layers as factors that shape businesses, but applying this approach is difficult because the Telecommunications Act does not yet recognize the layered model.74

Complicating the classification and policy effort is the fact that many traditional telephone services use VoIP technology because telecommunication service providers have incorporated IP networks within telecommunication networks.75 However, to “merely route traditional long distance traffic through a packet switch using Internet protocol and contend that it should not be subject to even terminating access charges” has been rejected by regulators.76 On the other hand, allowing a VoIP provider to connect calls to a regulated telecommunications network without paying regulated service rates may provide an “artificial competitive advantage over wireless and other wireline providers.”77

Like Congress, the FCC has not yet defined VoIP,78 but an FCC order has defined interconnected VoIP to “include any IP-enabled services offering real-time, multidirectional voice functionality, including, but not limited to, services that mimic traditional telephony.”79 The characteristics of interconnected VoIP are that: “1) the service enables real-time, two-way voice communications; 2) the service requires a broadband connection from the user’s location; 3) the service requires IP-compatible [customer equipment]; and 4) the service offering permits users generally to receive calls that originate on the PSTN and to terminate calls to the PSTN.”80 In addition, the FCC’s order stated the definition and characteristics of interconnected VoIP did not determine “whether a VoIP service that is interconnected with the PSTN should be classified as a telecommunications service or an information service under the Act.”81

The challenge of determining whether VoIP should be classified as an information service or a telecommunication service is underscored by “the danger of unintended and highly negative consequences”82 when regulators attempt to force new services into old categories.83 “Simply because something is functionally a substitute for something else, does not make it that something else.”84

VoIP in the Court—Making Lemonade out of Classification Lemons

VoIP’s most publicized service classification case is Vonage Holdings Corp. v. Minn. Pub. Utils. Comm’n.85 The Minnesota Public Utilities Commission (MPUC) received a complaint filed by the Minnesota Department of Commerce (MDOC) against Vonage, a VoIP service provider.86 The complaint requested Vonage be prohibited from marketing to potential Minnesota customers until Vonage complied with state regulatory requirements for the offering of telephone services.87 After a hearing, the MPUC ruled in favor of the MDOC’s request.88 Vonage then filed a complaint in the district court of Minnesota seeking a preliminary injunction.89
The issue that faced the court was whether Vonage may be regulated under Minnesota law that required companies to obtain certification before providing telephone services.\textsuperscript{90} Vonage asserted VoIP offerings were \textit{information services}, which were not subject to state regulation, and that the MPUC’s order was unconstitutional because the order violated the Commerce and Due Process Clauses of the Federal Constitution.\textsuperscript{91} In granting Vonage a permanent injunction against the order,\textsuperscript{92} the court reviewed the issue from several vantage points, and showed deference to congressional intent and FCC interpretations.\textsuperscript{93}

Based on statutory language, the court concluded that Vonage’s VoIP service satisfied the definition for information services, because “[t]he process of transmitting customer calls over the Internet require[d] Vonage to “act on” the format and protocol of the information.”\textsuperscript{94} Vonage \textit{transformed} the call formats and protocols required between VoIP and traditional telephone service users, and the court found that although Vonage \textit{uses} telecommunications services, Vonage does not \textit{provide} telecommunications services.\textsuperscript{95}

Based on the nature of the VoIP service, the court considered both phone-to-phone and computer-to-computer IP telephony. The court concluded Vonage’s VoIP service was not a telecommunication service because the service did not satisfy two of the FCC’s four conditions of IP telephony phone-to-phone.\textsuperscript{96} One condition was not satisfied because Vonage required customer premises equipment different from that used by traditional telephone service users, and a second condition was not satisfied because IP telephony content had to be converted “into a format compatible with the PSTN.”\textsuperscript{97} Vonage’s service was also ruled not to be a telecommunication service because within computer-to-computer IP telephony, the IP data packets did not travel through the PSTN.\textsuperscript{98}

The Vonage decision is instructive in how the court handled a converging telecommunication service that did not fit the Telecommunication Act’s existing classifications.\textsuperscript{99} The decision led others to observe that:

[in the constantly morphing world of new technology, what quacks like a duck may very likely also swim like a fish—so judges, business people and policymakers may argue ad nauseum which genus really fits (with their arguments almost inevitably colored by who will win or lose based on the ultimate classification). Convergence defies classification and challenges regulators to rethink the assumptions underlying current regulatory boundaries.\textsuperscript{100}]

With over 100 million Internet users in America, and with IP offerings competing with traditional telecommunication services, a coherent Internet policy framework is needed.\textsuperscript{101} Hopefully, future federal laws, court decisions, and FCC rulings “will reflect the best and brightest thinking in this complicated arena,”\textsuperscript{102} and will lead to new techniques of classification based on market competition.\textsuperscript{103}

Over time, the FCC will...need to shift its focus from specific regulatory approaches based on the particular technology platform—say, a distinct regimen for satellite, wireless, cable, or telephone networks—to a “layered model” of telecommunications regulation that regulates functionally similar services in the same way regardless of the underlying platform.\textsuperscript{104}

VoIP Security Policies

Congress stated the Internet should be regulation free, but also that public policy goals should “continue to apply as communications networks evolve.”\textsuperscript{105} National policies like 911-system access to public emergency services, and availability of voice communications to law enforcement, must be maintained.\textsuperscript{106} Although \textit{economic regulation} of telecommunication services should not apply to most IP-based information services,\textsuperscript{107} the lack of such regulations should not put information services “beyond the reach of regulations designed to promote public safety and consumer protection.”\textsuperscript{108}

The FCC’s challenge is to distinguish replacements for traditional telephone services, which raise law enforcement and emergency services policy concerns, from services that do not raise such policy and regulatory concerns.\textsuperscript{109} While VoIP services provide economic promise, “security issues must be addressed or [the] economic benefits could be lost in the wake of a malicious attack.”\textsuperscript{110} In addition, because emergency service providers and law enforcement agencies have based many programs on the PSTN and POTS, regulatory differences between telecommunication systems and information systems could render current programs ineffective as more users turn to VoIP services.\textsuperscript{111}
Emergency Services—Basic and Enhanced 911 Capabilities

VoIP Intersects with Emergency Services

Emergency services using 911 have existed since 1965.112 People do not care how a telephone works, but in an emergency, people expect that when dialing 911, the call will be answered, and emergency services can be dispatched to the appropriate location.113 In February 2005, the National Emergency Number Association estimated that 200 million calls to 911 were made annually, and that 911 service was available to almost 99 percent of the United States population.114

Requirements for 911 service are divided into “basic 911” and “enhanced 911” services.115 “Basic 911” service routes calls to an appropriate Public Safety Answering Point (PSAP),116 but does not define the type of information that must accompany the call.117 “Enhanced 911” (known as “E911”) requires communications service providers deliver the caller’s telephone number and location along with the routed call.118

The FCC ruled itself to have the authority “to determine whether the public interest required that a provider of a particular service should be required to provide 911/E911 to its customers, and if so, to what extent and in what time frame such covered service should be subject to the Commission’s 911/E911 requirements.”119 In determining whether a provider is subject to emergency service requirements, the FCC identified the criteria to be whether:

1) the entity offers real-time, two-way switched voice service, interconnected with the public switched network, either on a stand-alone basis or packaged with other telecommunications services; 2) customers using the service or device have a reasonable expectation of access to 911 and enhanced 911 services; 3) the service competes with traditional [commercial mobile radio service] or wireline local exchange service; and 4) it is technically and operationally feasible for the service or device to support E911.120

As recently as 2005, some VoIP providers did not offer 911 services, while other providers required prior customer activation of the service.121 When states responded by prodding VoIP providers to disclose 911 service capabilities to customers, some providers pointed to an FCC order122 that declared states may not regulate VoIP emergency service capabilities.123

Interconnected VoIP Intersects with Emergency Services

“Upon learning that some VoIP subscribers were having difficulties accessing emergency services, the FCC acted quickly and decisively to remedy the situation.”124 “In the Matters of IP-Enabled Services; E911 Requirements for IP-Enabled Service Providers”125 was adopted in May 2005, then released as an FCC order requiring interconnected126 VoIP service providers to supply customers with enhanced 911 service as a standard feature, whether customers are at or away from home.127

The FCC acknowledged a policy of “allowing these services to evolve without undue regulation in accord with our nation’s policies for Internet services,” while admitting an “obligation to promote ‘safety of life and property’ and to ‘encourage and facilitate the prompt deployment throughout the United States of a seamless, ubiquitous, and reliable end-to-end infrastructure’ for public safety.”128

E911 requirements do not apply to all VoIP services, but do apply to interconnected VoIP services.129 The FCC’s order allows interconnected VoIP providers to select from various methods to satisfy E911 requirements: “1) interconnecting to the E911 network indirectly through a third party, 2) interconnecting directly to the E911 network, or 3) employing any other method that allows them to provide E911 service.”130

3. VoIP Challenges within Emergency Services

E911 services are a complicated patchwork of regulations for all affected parties.131 States regulate traditional telephone service issues, while the FCC regulates wireless cellular issues, and PSAPs are local, while VoIP customers can be anywhere.132

VoIP providers are challenged to connect VoIP users to the appropriate PSAP133 because: “1) callers may not be able to connect to 911 dispatch centers; and 2) there is no guarantee that callers’ location information is correct when sent to a 911 dispatch center from a VoIP system.”134

How a VoIP provider connects to the PSTN may cause a customer dialing 911 to be connected with a fire or police department instead of the PSAP.135 To connect directly to the PSAP, the VoIP provider must interconnect with a local exchange carrier (LEC), but “[s]ome LECs have refused to cooperate with VoIP services in providing 911 access.”136 To address connectivity concerns, some VoIP services display a disclaimer regarding emergency services limitations, and some VoIP providers recom-
mend maintaining traditional telephone services at the caller’s physical location. 137

Although regulations may require an interconnected VoIP provider to have a “method for determining a user’s location
without assistance from the user,” 138 a first step is to require VoIP providers to retain, for each customer, a default location,
which is “the physical location at which the service will first be utilized.” 139 A permanent solution will likely be based on real
time determination of location using “cellular tower triangulation, where location is measured based on the signal strength to
multiple cellular towers.” 140 Triangulation technology may improve existing emergency service offerings, and become a com-
petitive advantage over traditional telephone services, giving VoIP providers an incentive to invest in emergency service capa-
bilites. 141 Looking ahead, the National Emergency Number Association listed six recommendations for improving emergency
access for customers of IP-based services:

1) establishing a national E9-1-1 VoIP policy; 2) encouraging vendor and technology neutral solutions and innova-
tion; 3) retaining consumer service quality expectations; 4) supporting a dynamic, flexible, open architecture system
design process for 911; 5) developing policies for 911 compatible with the commercial environment for IP communi-
cations; and 6) promoting a fully funded 911 system. 142

Wire Tapping—Law Enforcement Access to VoIP Communications

VoIP Intersects with Wire Tapping

A significant Department of Justice concern regarding VoIP is that the technology must not become a refuge for “criminals,
terrorists, and spies” 143 because law enforcement is unable to access VoIP communications. 144 Law enforcement has become
accustomed to the ease of “tapping voice communications for eavesdropping purposes,” 145 and the effectiveness of electronic
surveillance in fighting “terrorism, espionage, and organized crime.” 146 The Federal Bureau of Investigation (FBI) is pushing for
updated Internet eavesdropping rules that allow access to VoIP calls, as well as electronic mail, Internet browsing, and instant
messaging, although that request concerns some privacy and civil liberty advocates. 147

Today, law enforcement can legally intercept any Internet communication, including VoIP transmissions, under Title III of
the Omnibus Crime Control and Safe Streets Act of 1968, under the Electronic Communications Privacy Act of 1986, or under
the Foreign Intelligence Surveillance Act of 1978. 148 For example, the FBI has served Vonage with subpoenas for call records and
data maintained by Vonage. 149 In addition to call records and data, because all VoIP transmissions pass through provider servers,
providers may be able to copy the communication data packets (which contain call content) for law enforcement use. 150

The FBI is concerned because the technologies for intercepting VoIP and traditional telephone calls differ, and in addition,
the ease with which strong encryption can be applied to VoIP transmissions may prevent law enforcement from accessing call
content. 151 For these reasons, law enforcement agencies may need to master the numerous formats and protocols used by VoIP
providers, and work with multiple providers to intercept a single VoIP transmission. 152 The Department of Justice warned that
future VoIP regulation must consider:

1) That public safety and national security will be compromised unless court orders for electronic surveillance can be
implemented by providers; 2) that assistance requirements should apply to every service provider that provides switch-
ing or transmission, regardless of the technologies they employ; and 3) that if any particular technology is singled out
for a special exemption from these requirements that technology will quickly attract criminals and create a hole in law
enforcement’s ability to protect the public and the national security. 153

VoIP Intersects with the Communications Assistance for Law Enforcement Act

“Currently, most forms of electronic surveillance are governed by the Communications Assistance for Law Enforcement Act
(CALEA),” 154 which sets telecommunication provider requirements for interception of targeted communications, and provides
law enforcement agencies with access to intercepted communications by way of a court order or other appropriate authoriza-
tion. 155 CALEA was intended to preserve the ability of the government to intercept wireless or digital transmissions, regardless
of whether advanced features such as speed dial, conference calling, or call forwarding were in use. 156 Public policies which CA-
LEA attempts to balance are: “1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly
authorized intercepts; 2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and 3) to
avoid impeding the development of new communications services and technologies.” 157
Regardless of whether VoIP is classified as an information service or communications service, law enforcement believed that application of CALEA to IP-based communications “would be in the best interests of the public.” Therefore, the FBI and Department of Justice petitioned the FCC to extend CALEA to all Internet communications. The FCC responded that CALEA applied to interconnected VoIP service providers and targeted compliance for May 2007. The FCC later ruled that service providers would be responsible for CALEA compliance costs, and declined to institute a national surcharge to recover the costs, as the surcharge would not serve the public interest.

All parties generally agree that law enforcement interests should be balanced with national interests in promoting communications technology innovation, as well as balancing interests in “maintaining American leadership of Internet technology development, expanding access, keeping costs down, enforcing competition, protecting privacy, and enhancing network security.” How providers will cooperate and interact to comply with CALEA requirements is not clear. VoIP technology separates the voice application from the transmission network, and while the VoIP provider may be able to provide call routing information, the network provider may need to be involved to gather call content information. Commentators have argued against giving law enforcement the authority to demand design obligations from VoIP providers, claiming the ability “to impose technology design mandates would chill technological innovation and drive technology development out of the U.S.” Another concern regards the additional, and far more private, content information available through VoIP interception. In traditional telephone call interception, “law enforcement receives details about when a phone call was initiated, but receives neither the content of the call nor any information about the call,” but for VoIP communications, the ease of copying data packets may entice law enforcement to request information regarding the subject of the call. There is also risk that “rogue employees of the service providers could abuse the internal surveillance capability.”

VoIP security policies are in a state of transition, and given the FCC’s reluctance to regulate information services, market forces will play a significant role in defining the framework for VoIP security. As VoIP services replace traditional telephone services, the threat of tort liability may drive some VoIP providers to ensure security offerings, such as E911 services, are deployed. The federal government has several options to affect VoIP security concerns, including the government’s purchasing power, federal tax incentives, and the legislation of security requirements (such as how providers shall comply with CALEA). “However, given that the market for VoIP services is still evolving, such requirements might be both premature and in fact harmful for the future implementation of such services.”

Conclusion

Over the past 12 years, VoIP has developed from a novel gimmick, to the brink of becoming the dominant worldwide transport mechanism for voice communications. In April 2007, a Google search of “VoIP Revolution” produced over 450,000 results. Traditional telephone services will not disappear anytime soon, but analog services are being hybridized as communications providers increase the use of IP-based technologies to lower the cost of pushing telephone calls.

Business users are enticed by the possibility of converging data and voice networks, integrating voice and e-mail communications, and locating people who use IP-based devices. Individuals appreciate lower monthly bills, portable “telephone” numbers, and being able to make calls wherever a broadband connection can be found. VoIP is not without technological disadvantages, but neither a reliance on electricity nor a vulnerability to malicious electronic attack shall prevent the telecommunication industry’s transformation.

As VoIP enters its challenging teenage years, look for Congress to redefine public policies regarding communications. In response to new legislation, expect the FCC to identify new approaches and regulations that promote revised national objectives, goals, and concerns. As part of VoIP’s growing pains, challenges like 911-system access to emergency services and law enforcement’s access to voice communications are being addressed by regulators, providers, and customers, whose demands are balanced while ensuring public safety and consumer protection.

Many people will have a natural hesitancy to convert from tried and true “plain old telephone service” to state-of-the-art VoIP, but if it’s good enough for criminals, terrorists, and spies, it’s good enough for me!

Endnotes

1 Paula K. Royalty, When is a Phone Call not a Phone Call? Legal Issues Arising from Business Use of VoIP, 1 SHIDLER J. L. COM. & TECH. (2004).
Id. at 1. “Early ventures in peer-to-peer IP telephony were largely unsuccessful in part due to the nature of early IP networks, which offered limited reliability and voice quality. Today, however, as a result of improvements in technology, IP networks are increasingly being used to carry voice communications.” In the Matter of IP-Enabled Services, 19 FCC Rcd. 4863, 4871-73 (2004).


Emily Frye & Gregory Staita, Hold the (Internet) Phone! The Implications of Voice-over-Internet Protocol (VoIP) Telephony for National Security & Critical Infrastructure Protection, 1 ISJLP 571, 571-72 (2005). “But VoIP services are not necessarily mere substitutes for traditional telephony services, because the new networks based on the Internet Protocol are, both technically and administratively, different from the PSTN.” 19 FCC Rcd., at 4866.

Frye & Staita, supra note 4, at 572.

Id. “[M]ore and more businesses are moving to VoIP solutions in lieu of PBXs and other traditional facilities to manage their communications.” 19 FCC Rcd., at 4866 n.6.

Frye & Staita, supra note 4, at 572. IP challenges the assumptions on which communications networks and regulations are based. “Packets routed across a global network with multiple access points defy jurisdictional boundaries. Networks capable of facilitating any sort of application that programmers can devise have empowered consumers to choose services they desire rather than merely accepting a provider’s one-size-fits-all offering.” 19 FCC Rcd., at 4866-67.


Frye & Staita, supra note 4, at 573.

Ellig & Walling, supra note 8, at 92.


Ellig & Walling, supra note 8, at 93. An Internet Service Provider (ISP) exemplifies information services, as ISPs allow consumers to exchange information by way of the Internet, enabling “consumers to process and store the data in various ways.” Winstanley, supra note 12, at 539.


Id. at 165-66.

Id. at 166.

Id.

Id. “According to industry data compiled by the Commission, interstate access minutes have declined significantly in recent years; industry watchers expect VoIP to hasten the decline.” In the Matter of IP-Enabled Services, 19 FCC Rcd. 4863, 4866 n.11 (2004). See also Remarks of Commissioner Robert M. McDowell; Before the National Telecommunications Cooperative Association (NTCA), Orlando, Florida, 2007 FCC LEXIS 1147, *5, which noted that “the number of wireline switched access lines has declined from around 192 million in December 2000 to 175 million in December 2005,” and identified “an increase in VoIP subscribers from 150,000 in 2003 to 4.2 million in 2005.”


Leonard J. Kennedy & Heather A. Purcell, Wandering Along the Road to Competition and Convergence - The Changing CMRS Roadmap, 56 Fed. Comm. L.J. 489, 558 (2004). “IP-enabled services generally -- and VoIP in particular -- will encourage consumers to demand more broadband connections, which will foster the development of more IP-enabled services. IP-enabled services, moreover, have increased economic productivity and growth, and bolstered network redundancy and resiliency.” 19 FCC Rcd., at 4867.


"Id. at 583. ‘Furthermore, with the increased availability of ‘user-friendly tools’ to conduct DoS attacks, even ‘less knowledgeable’ hackers [can] conduct attacks with relative ease.’ Id. at 585.

"Id. at 582.

"Id.

"Id. at 583.

"Id. at 587.

"Id.


"Id.

"Id.


"Bythe, supra note 42, at 165.


"Id. at 558-59.

"Id. at 558.

"Id. at 559.


"Id. at 5.


"Id. at 171.

"Id.


"Nakahata, supra note 56, at 172-73.


"Id. at 499.

"Id. at 485.

"Id. at 499.

"Id. at 485.

"Id. at 484.

"Id. at 485.

"Id. at 499.

"Id. “The inherent flexibility of IP-based transmission to deliver multiple services has led several commentators to call for what has come to be called a ‘layered’ approach to analysis of regulation. Although different commentators have used varying numbers of layers, one of the most common is a four-layered model of content, application, code/logic, and physical.” John T. Nakahata, *THE JOURNEY TO CONVERGENCE: CHALLENGES AND OPPORTUNITIES: SYMPOSIUM ON DIGITAL MIGRATION - HOSTED BY COMMLAW CONSPECTUS, INSTITUTE OF COMMUNICATIONS LAW STUDIES, AND THE FEDERAL COMMUNICATIONS COMMISSION: Symposium Article: Broadband
“While we adopt no formal definition of ‘VoIP,’ we use the term generally to include any IP-enabled services offering real-time, multidirectional voice functionality, including, but not limited to, services that mimic traditional telephony.” In the Matter of Petroff v. BT, 19 FCC Rcd. 7457, 7457 (2004). The FCC ruled AT&T’s use of VoIP was a telecommunications service because “end-user customers do not order a different service, pay different rates, or place and receive calls any differently than they do through AT&T’s traditional circuit-switched long distance service.” Id. at 7465.

“In using the term ‘phone-to-phone’ IP telephony, we tentatively intend to refer to services in which the provider meets the following conditions: (1) it holds itself out as providing voice telephony or facsimile transmission service; (2) it does not require the customer to use [customer premises equipment] different from that [ ] necessary to place an ordinary touch-tone call (or facsimile transmission) over the public switched telephone network; (3) it allows the customer to call telephone numbers assigned in accordance with the North American Numbering Plan, and associated international agreements; and (4) it transmits customer information without net change in form or content.” In the Matter of Federal-State Joint Board on Universal Service, 13 FCC Rcd. 11051, 11543-44 (1998).


20 FCC Rcd., at 10248.

19 FCC Rcd., at 4898.

Id. E911 deployments are still in process across the United States. Id.

Id. at 4899.

Id. at 4900.


Brannon, supra note 121, at 198.

Id.


"[I]nterconnected' refers to the ability of the user generally to receive calls from and terminate calls to the public switched telephone network (PSTN), including commercial mobile radio service (CMRS) networks.” Id. at 10246 n.1.

Id. at 10246. The FCC’s sense of urgency is highlighted in a footnote that stated the interconnected VoIP E911 order was released in advance of other IP-Enabled service issues, because the Commission sought to address public safety concerns. “For example, [the Commission was] aware of a recent incident in Texas in which it was reported that a 911 call was not completed when an interconnected VoIP user dialed 911 to seek emergency assistance during a home invasion burglary.” Id. at 10246 n.2.

Id. at 10247.

Id. note 121, at 199.

Id. at 200.

Id. at 192.

Id.


Id. at 578.


Frye & Staita, supra note 133, at 578.


Id. at 199-200. “VoIP providers have initially managed this by simply having subscribers register where they would be making their calls from. Registration can be changed easily and updated within hours of moving.” Ellig & Walling, supra note 135, at 131.

John B. Morris, Jr., 2004 PRIVACY YEAR IN REVIEW SPECIAL TOPIC: VoIP: Privacy Year in Review: Privacy and VoIP Technology, 1 ISJLP 509, 515 (2005). Location can be determined using a global positioning system within a computer or mobile telephone. “In some parts of the world wireless services providers are already ‘pushing’ advertisements to phones based on the location of the phone (and thus the location of the user).” Id.

Frye & Staita, supra note 133, at 579.

Brannon, supra note 138, at 193.

Id. at 188.

Id.

Id.

Id.

Paula K. Royalty, When is a Phone Call not a Phone Call? Legal Issues Arising from Business Use of VoIP, 1 SHIDLER J. L. COM. & TECH. 1 (2004).


Id.

Id.

Id.

Id.


Id. at 189.


Brannon, supra note 153, at 189.

Id.

Id.

Id.

Id.

Id.

Id.


Brannon, supra note 153, at 190-91.

CALEA labels call routing information as ‘call-identifying information’ which is defined as “dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunication carrier.” Jerry Ellig & Alastair Walling, Regulatory Status of VoIP in the Post-Brand X World, 23 Santa Clara Computer & High Tech. L.J. 89, 130 (2006).


Id.

Id.

Id. at 515.

Frye & Staita, supra note 164, at 595.

Id.

Id at 595-96.

Id.


The latest Internet phenomenon

The exceptional rise of computer usage today, and the Internet with its ease of faceless interaction, have created a new type of tyrant: the cyber-bully. The online environment now allows extensive interactions using computer means such as e-mail, websites, blogs, instant messaging, chat rooms, and even text messaging to cellular telephones. This type of communication allows anonymity, and thus, many feel more inclined to do things in Internet forums that they would normally not do in traditional social settings. As with the conventional form of bullying, this online adaptation manifests itself in everyday society, but particularly in the adolescent world as an extension of “school yard” exchanges.

While bullying, in general, is socially viewed as unacceptable behavior based on both verbal and physical elements, the cyber version can go largely unnoticed. Using electronic media, it can be for the most part undetectable by outsiders unless the victims of such attacks step forward. Even when the victims do alert to these issues, it is often problematic to identify the online aggressor. Furthermore, with the Internet as an encouraged forum for free speech, government regulation of Internet activities is quite difficult without causing a chilling effect on acceptable online expression. There is a further debate as to the extent of control or authority that educational facilities have balanced with the free speech protections of students when the Internet exchanges occur off-site from the school.

The purpose of this discussion is to view areas of online behavior that are included in the scope of “cyber-bullying” specifically related to the educational environment, the applicability of current laws or court decisions in regulating such activities, and other protections that may exist.

“Cyber-Bullying” Defined

The term “cyber-bullying” first appeared in federal courts in 2001 in a case involving unfair competition by trademark misuse. The plaintiffs alleged “an admittedly new and unrecognized cause of action: cyberbullying.” The claim was denied, and the “cyber-bullying” term has since taken on a more common meaning: one indicating an activity directed personally at individuals.

“Cyber-bully” has been used to encompass various unwanted activities online, including bullying, threatening, harassment, and stalking. Wikipedia defines the term “cyber-bully” as “refer[ing] to bullying and harassment by use of electronic devices through means of e-mail, instant messaging, text messaging, blogs, mobile phones, pagers, and websites.” Alternative definitions include “willful and repeated harm inflicted through the medium of electronic text” and “the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging, defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others.” While other formal and informal definitions of both “cyber-bullying” and “cyber-harassment” are avail-
able, for the purposes of this discussion, the distinction will solely involve the intended online victim: the fellow student or the educational professional.

In the educational environment, “cyber-bullying” is typically used to refer to activities on the Internet or wireless media of one school peer against another. Such examples could include posting demeaning comments on websites, sending harassing communications directly to the victim, posting cruel images, broadcasting embarrassing material, and even pretending to be the victim online in order for the target to be looked upon negatively. The activity can also take on a sexual harassment nature, for example, when adolescent boys post sexual details regarding fellow female classmates. In contrast, “cyber-harassment” is commonly used to describe online activity by students targeting teachers or other educational professionals. The typical format involves websites where students can post negative comments. While this may seem to be only an expression of opinion by the students, harmful messages such as those alleging sexual abuse or other indiscretions could jeopardize the employment and future of these educational professionals.

The only similar term to online bullying that seems to have a formal legal definition is “cyberstalking.” It has been described as:

> [t]he act of threatening, harassing, or annoying someone through multiple e-mail messages, as through Internet, especially with the intent of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient or a member of the recipient’s family or household.7

Various state statutes provide alternate definitions of cyberstalking, including Illinois where the action is described as “knowingly and without lawful justification, on at least two separate occasions, harasses another person through the use of electronic communication” with a threat to cause harm or reasonable apprehension of such harm. As these definitions are quite broad to encompass various forms of bullying and harassment online, this may allow the applicability of some state statutes prohibiting cyberstalking to situations of bullying in a school setting.

Although common to our vocabulary, traditional bullying also does not have a known legal definition. Wikipedia describes it as “the tormenting of others through verbal harassment, physical assault, or other more subtle methods of coercion such as manipulation.”8 Although the method has changed from the traditional sort to the online version, the intent remains the same: to exercise power over another. While both stem from relationships formed at school, the cyber-bully can exercise bullying activities outside of the schoolyard and classroom. In fact, cyber-bullying can occur completely outside of the physical geographic region of the school, making it that much more difficult to detect and control via applicable laws.

**Why Cyber-Bullying?**

When one thinks of a schoolyard bully, the perception is a stronger child with the physical power to be threatening to other students. Another form would be in the popularity circle where social acceptance takes the place of physical power for the bullying action. The Internet offers a whole new form of power over another for the purposes of bullying; via the ability to effectively use electronic media and navigate the Internet. Employing a wide range of Internet communication tools, the technologically savvy student, neither popular nor strong, can be in the power position compared to victims. 9

Communicating online allows the user to remain anonymous. Many websites offer free e-mail and instant messaging accounts whereby one can sign up without giving any factual information regarding true identity, for example, Yahoo!® and MSN® Hotmail, and their associated instant messaging programs. Thus, even if a victim of cyber-bullying wished to report the offender, it may be virtually impossible to determine his identity and location. Because of this online anonymity, the aggressor student feels he can victimize another student without fear of reprisal.

Furthermore, there is little supervision over an adolescent who is actively participating in the cyber world. Short of some of the parental control software, youths can navigate various chat rooms, websites, peer-to-peer transfer sites, and so forth, without the watchful eye of parents. In general, parents may think that their child is safely utilizing the Internet because the parental controls have not detected obscene website access attempts, and not realize that there have been activities of bullying or of being bullied. It is also more commonplace for parents to provide their children with their own workstation, sometimes in a shared area of the household and even a dedicated computer in the bedroom, again making detection of unwanted cyberspace behavior that much more difficult to recognize.

Furthermore, the ability to target the victim both inside and outside the school environment could be particularly appealing
to the cyber-bully. The notion of a continuous bully has become a reality thanks to the communication possibilities of cyber-space. Adolescents can target their peers both during school hours and persistently continue the behavior when the victims return home, even under their parents’ supervision. Therefore, the victim can feel that he/she is never out of the reach of the bully and in a sense, is a “perpetual target.”

Cyber-bullying through the use of Internet communication can be confidential, from aggressor to victim. Although widely visited websites are one method of bullying online, private communication between two user accounts can be a preferred method for lacking control. For example, a computer proficient adolescent can quickly learn methods to remain anonymous or to cover the tracks of any online interaction. Again, this makes parental detection or control more unlikely. In addition, many adolescents may feel that online activity is free speech, and thus they feel no threat of repercussion.

The Free Speech Debate

Regulating Internet activities has a particular challenge with respect to the constitutional right to free speech. The First Amendment of the United States Constitution provides that “Congress shall make no law . . . abridging the freedom of speech.” Of course, it is known that this text does not mean that all speech is protected. Clearly, there are some forms of speech that are not afforded the protection of the First Amendment. However, even areas of speech or conduct not falling within the protections can be challenged should the laws regulating it, having a chilling effect on speech that is protected.

Imprecise laws can be attacked on their face under two different doctrines: first, the overbreadth doctrine permits the facial invalidation of laws that inhibit the exercise of First Amendment rights if the impermissible applications of the law are substantial when judged in relation to the statute’s plainly legitimate sweep; second, even if an enactment does not reach a substantial amount of constitutionally protected conduct, it may be impermissibly vague because it fails to establish standards for the police and public that are sufficient to guard against the arbitrary deprivation of liberty interests.

The overbreadth issue surfaces when a statute is overbroad such that is has the affect of punishing both protected and unprotected speech. However, “the overbreadth scrutiny diminishes as the behavior regulated by the statutes moves from pure speech toward harmful, unprotected conduct.” In terms of vagueness, “[i]t is established that a law fails to meet the requirements of the Due Process Clause if it is so vague and standardless that it leaves the public uncertain as to the conduct it prohibits.” In summary, regulation of online speech proves to be a continuing complexity for which Congress must tread carefully when enacting any possible laws so as to survive the constitutionality challenge.

With respect to the public school system, the Supreme Court ruled in 1969 in Tinker v. Des Moines Independent Community School District that “[i]n [the] absence of specific showing of constitutionally valid reasons to regulate their speech, students are entitled to freedom of expression of their views.” This means that although students may not share the same open rights of free speech within the confines of the public school system, they are not in complete absence of such rights. The standard set out in Tinker is that facts must be demonstrated “which might reasonably [lead] school authorities to forecast substantial disruption of, or material interference with, school activities or any showing that disturbances or disorders on school premises” exists in order for expression to be controlled by school officials. However, this case involved silent student political demonstrations protesting the Vietnam War and not activities such as bullying and harassment.

In 1986, the standard for the public school system slightly changed due to a student’s delivering a nomination speech in a school assembly laced with sexual language. It was held in Bethel School District Number 403 v. Fraser that the “school district acted entirely within its permissible authority in imposing sanctions upon student in response to his offensively lewd and indecent speech, which had no claim to First Amendment protection.” The Court found that such speech could be regulated by the school officials because it “undermine[d] the school’s basic educational mission.” This new Fraser standard recognizes the “necessity of balancing the right to free speech with the goal of protecting the rights of others where speech causes harm.”

The case of Hazelwood School District v. Kuhlmeier further refined the standard in 1988. The question required the Court to determine whether the First Amendment protected speech that was developed within a school sponsored activity using school resources where the public school authorities had found it to be objectionable. Here, the principal had censored articles from the school newspaper, deeming a pregnancy article with sexual references unsuitable for younger students. The Supreme Court held that the “high school paper that was published by students in journalism class did not qualify as ‘pub-
lic forum,’ so that school officials retained right to impose reasonable restrictions on student speech in paper.”24 Thus, school sponsored expression is not fully protected by the First Amendment. However, as seen in a similar situation in Dean v. Utica Community Schools in 2004, this exercise of editorial control is not limitless. The “control over the style and content of student speech in school-sponsored expressive activities” must be “related to legitimate pedagogical concerns.”25

While the three landmark cases, Tinker, Fraser, and Kuhlmeier, all provide clear but distinguishing standards for regulating speech in the school system, they are not entirely applicable to the situation of cyber-bullying. Each of the above cases referenced activities that occurred within the confines of the school. If online bullying and harassment were to occur solely within the bounds of the school using school resources, undoubtedly the standards would strictly apply. However, although cyber-bullying activities may stem from relationships formed in the educational environment, the actual events typically result from computer use outside the walls of the school buildings. Today, many families own or have access to a personal computer and the Internet, and many children have accessibility in the privacy of their own bedrooms outside of the prying eyes of their parents. Therefore, the question becomes whether speech which would normally be outside First Amendment protections while in school is also unprotected when not in school.

In 2000, a United States District Court granted a temporary restraining order preventing the suspension of a Washington student regarding a website that he published off campus showing a “death list” of fellow students.26 Here, because the student claimed the list to be no more than a joke or parody of a class assignment requiring students to write their own obituary, the court held that the “student had a substantial likelihood of success on the merits of his claim that [the] school violated his First Amendment rights.”27 Since there was no evidence that the mock obituaries were intended to threaten anyone or that anyone was actually threatened by them, combined with the website’s having been created off-campus without the use of school resources, there was insufficient proof that the activity would have the effect of disrupting the educational environment.28 Again in 2002, the United States District Court held that a Michigan student’s suspension had violated his First Amendment rights to free speech. Here, the student had published a website off-campus listing people from his school that he “wished would die,” although he claimed it to be no more than a joke.29 The court found that “absent proof of disruption to school by website or that website was created on school property,” the school-imposed penalty was constitutionally unwarranted.30

In contrast, courts have found sufficient connection between off-campus activities to allow school policies to take effect without interference from a constitutional challenge. Although not directly related to Internet speech, one example shows a court’s willingness to allow school disciplinary action to be effective. In 1989, a Massachusetts student had committed battery on a fellow student off the school property, but extending from incidents and planning which had occurred earlier that day on school property.31 Although the Court declined to discuss the distinction between on- and off-campus conduct, it held that the student’s rights were not violated.32 Again in 2000, the state court found that the free speech protections of a Pennsylvania student were not violated when the school district had permanently expelled him for the creation of a “website containing threatening and derogatory comments about [a] teacher and principal.”33 Here, the court reiterated the ability of the “courts [to] recognize the authority of school officials to discipline students for off-campus activity where that activity materially and substantially interferes with the education process.”34 Similarly, the Wisconsin State Court has also found that school authorities may discipline students for off-campus activities where the “misconduct for which the pupils were suspended [is] such as to have a direct and injurious effect upon the good order and discipline of the school.”35 A poem written by the students had found its way into a public newspaper which the school district believed was “detrimental to the interests of the school: that it not only tended to hold up said school, its discipline, and its teachers to public contempt and ridicule, but it also tended toward awakening in the minds of the pupils themselves a feeling of hostility toward the teachers and a defiance toward the proper control and management of the school.”36 The court reasoned that the publication of this poem, because it found its way into the homes of many of the students, “would be as much influ[en]tial thereby as if the writing had been printed and posted in the schoolroom, or there circulated and read.”37

In determining the interference allowed by school authorities for off-campus speech and conduct, the courts have looked to a close nexus between off- and on-campus activities. Where such a close connection is found, “[t]he school authorities must necessarily be invested with a broad discretion in the government and discipline of the pupils, and the courts should not interfere with the exercise of such authority unless it has been illegally or unreasonably exercised.”38 However, where the connection is found to be minimal, free speech protections of the First Amendment will extend to students engaged in off-campus Internet activities. “[B]ecause school officials have ventured out of the school yard and into the general community where the freedom
accorded expression is at its zenith, their actions must be evaluated by the principles that bind government officials in the public arena.”

Unlike on-campus activities, school control over on-campus speech is necessarily narrower; thus, “courts impose a heavy burden on schools to show sufficient disruption to regulate off-campus speech.”

Since adolescent cyber-bullying commonly extends from relationships established in the educational environment and will have a likely impact on the student victims, it is plausible that the courts could reasonably find a nexus sufficient to allow school district authority over such cyberspace speech. Bullying, in its traditional sense, has long been known to be disruptive to the educational process due to its detrimental effects on the victims. Thus, with cyber-bullying being another form of this traditional aggressive behavior, it can be reasoned that the Tinker standard requiring the “forecast [of] substantial disruption of, or material interference with, school activities or any showing that disturbances or disorders on school premises” will be adequately satisfied.

Accountability

While exercising governmental or school authority over cyber-bullying activities may prove to be a burdensome task, another approach would be to seek damages for those harmed by the activities. Who should be held accountable for the harm caused by online bullying or harassment? One could ascribe some responsibility on the Internet service providers, the educators or public school officials, or even parental liability over the activities of the cyber-bully aggressor. However, although damages may seem warranted, assigning the accountability can prove to be as cumbersome as regulating the actions which inflicted the harm in the first place.

Internet service providers (ISPs) provide individual accounts for accessing the Internet. Some believe that ISPs should be held liable for defamation where they have allowed individuals who use their systems to send libelous or improper electronic messages. However, a counter argument is that it would be unreasonable to require ISPs to regulate all electronic traffic through their respective networks, and even if possible, would curb the free speech enjoyed through Internet media. Even so, ISPs require service agreements from its customers to shield themselves from liability from any improper use. For example, the following provisions are included in the terms of use for a popular ISP:

YOUR AFFIRMATIVE ACT OF USING AOL.COM SIGNIFIES THAT YOU AGREE TO THE FOLLOWING TERMS OF USE, YOU CONSENT TO THE INFORMATION PRACTICES DISCLOSED IN THE AOL NETWORK PRIVACY POLICY, AND YOU CONSENT TO RECEIVE REQUIRED NOTICES AND TO TRANSACT WITH US ELECTRONICALLY. IF YOU DO NOT AGREE, DO NOT USE AOL.COM.

and

You agree that we are not liable for Content that is provided by others. We have no duty to pre-screen Content, but we have the right to refuse to post or to edit submitted Content. We reserve the right to remove Content for any reason, but we are not responsible for any failure or delay in removing such material.

This type of agreement provides indemnification of the ISP from the actions of its users, yet reserves the right to filter content at its discretion. In order to gain access to the Internet through the ISP’s network, terms of use such as the above must be agreed to. The user is provided an alternative to the terms, and that is to not use the ISP. Furthermore, in 1999, the Court of Appeals of New York held that an ISP “was not the ‘publisher’ for defamation purposes, of e-mail and electronic bulletin board messages” sent by an imposter who was pretending to be the plaintiff via a falsely opened account.

In addition to the ISPs, there are many websites that offer various Internet communication forums where individuals can effectively have their own web pages and electronically communicate through “friends” networking. These include, but are not limited to, MySpace.com®, Facebook©, and myYearbook©. Like the ISPs, these social networking websites also require users to accept terms of use, or not use the services provided. For example, the following provisions are included in the terms of use agreement for both registered users and guests of the MySpace.com® website:

MySpace.com may delete any Content that in the sole judgment of MySpace.com violates this Agreement or which may be offensive, illegal or violate the rights, harms, or threaten the safety of any person. MySpace.com assumes no responsibility for monitoring the MySpace Services for inappropriate Content or conduct.
Prohibited activity includes, but is not limited to: criminal or tortious activity, including child pornography, fraud, trafficking in obscene material, drug dealing, gambling, harassment, stalking, spamming, spimming, sending of viruses or other harmful files, copyright infringement, patent infringement, or theft of trade secrets . . . 46

Again, the websites require users to agree to release them from liability for any content posted by other users, although it retains the right to remove content at their discretion. Very recently, in February 2007, a district court in Texas dismissed the claims of negligence and gross negligence against the website owner by the mother of minor who was the victim of a sexual predator through the use of the networking website. 47 Here, the court held that the “immunity provision under Communications Decency Act (CDA) applied to negligence and gross negligence claims that operator knew that sexual predators were using service to communicate with minors and did not react properly.” 48 The CDA of 1996 provides that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” whereby an interactive computer service includes “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server.” 49 Clearly, social networking websites fall within the definition of “interactive computer service,” and thus the owners do not have a duty to institute measures to protect individuals or filter online content used on their sites.

However, unlike the ISPs and website owners, educational facilities do not share the same shields from liability. It was held by the Supreme Court in 1999 that “a private damages action may lie against a school board under Title IX in cases of student-on-student harassment, but only where the finding recipient acts with deliberate indifference and the harassment is so severe that it effectively bars the victim’s access to an educational opportunity or benefit.” 50 Although the case involved sexual harassment of a student, the holding is easily applicable to bullying circumstances. Furthermore, if a sufficient connection can be made to the off-campus Internet activity, thereby giving the school the authority to regulate such activity, private damages actions may also surface successfully for cyber-bullying circumstances. Thus, if it can be proven that there was actual knowledge and the school authorities deliberately did not take action to investigate or stop the harassment or bullying, the school district may be liable for damages for harm caused to a student by cyber-bullying.

Parents can also be held accountable for the actions of their children. Many terms of use agreements for ISPs even include provisions that the account holder is responsible for the actions of all parties in the household, including minors, who use the Internet access account. “Many states have enacted statutes making parents responsible for damages caused by willful, malicious, intentional, or unlawful acts of their minor children. These statutes have been held constitutional, though there is authority to the contrary.” 51 Typically these statutes are directed at destruction of property, operation of a motor vehicle, and so forth. Given online bullying is a relatively new development, it will be interesting to see how the courts will interpret the state laws for parental liability for the unlawful acts of their children engaged in online harassment.

What Legal Protections Exist?

While seeking damages for the harm caused by cyber-bullying is one remedy, the focus should really be on prevention. In August 2006, Congress passed legislation to authorize grants to “combat domestic violence, dating violence, sexual assault, and stalking in middle and high schools” referred to as the “Supporting Teens through Education and Protection Act of 2005” or the “Step Act.” 52 This allows the attorney general to provide funding to middle schools and high schools that are working with various experts to combat the problem of violence and sexual assault so as to allow them to provide training, support, etc. Specifically, eligibility can include “organizations and service providers addressing sexual harassment, bullying, or gang-related violence in schools.” 53 Effective January 2006, Congress had also passed legislation to offer grants to states for the “purpose of strengthening the juvenile justice system” through various methods. 54 Specifically included in the statutory provisions is funding for “establishing and maintaining accountability-based programs that are designed to enhance school safety, which programs may include research-based bullying, cyberbullying, and gang prevention programs.” 55

Various states have been actively pursuing legislation to address harassment and bullying in the educational system. For example, in Texas there is a pending house bill entitled “Corrine’s Law” that would amend the current state education code to add a subchapter on harassment. 56 The definition offered for harassment includes “expression[s] made through electronic medium” and details the intended targets as “student or school employee or volunteer,” 57 which appears to encompass the problem
of adolescent cyber-bullying stemming from relationships developed at school. The proposed text further provides that the “physical location or time of access of an act of harassment made through a computer, computer network, or other electronic medium may not be raised as a defense in a criminal action or disciplinary proceeding relating to the act of harassment,”68 a notable attempt to blur the distinction of on and off-campus speech. However, this provision stands the test of whether there is a sufficient nexus and associated resultant effects as required by the standard detailed in 

Tinker59 and Fraser60 so as to allow educational environment authority and escape the protections of free speech of the First Amendment.

Florida is also reviewing proposed state legislation relating to school safety in a house bill entitled “Jeffrey Johnston Stand Up for All Students Act.”61 Named on behalf of a 15-year-old student who killed himself in June 2005 after being tormented by Internet postings from middle school classmates,62 the act has the purpose of prohibiting bullying or harassment of students or school employees. Jeffrey hung himself by his book bag strap in the bedroom closet after enduring three years of persistent Internet bullying which depicted him as a “faggot, a stalker and a creep.”63 Jeffrey’s mother admits that the she was aware of the bullying of her son online, but was powerless to stop it or have the school take action, even though she was herself a teacher.64 The act requires that each school district adopt policies to prohibit bullying and harassment, and includes provisions that allow for disciplinary action even when a computer is used from home against a fellow student or school employee.65 In addition, the school policies must include reporting, investigation, and disciplinary action guidelines. Like the Texas proposal, the Florida house bill includes that the “physical location or time of access of a computer-related incident cannot be raised as a defense in any disciplinary action or prosecution initiated under this section,”66 thus targeting the issue of cyber-bullying. However, as previously detailed, such future legislation cannot violate the free speech protections, and this bill specifically states as such in its final provision indicating that “[n]othing in this section shall be construed to abridge the rights of students or school employees that are protected by the First Amendment to the Constitution of the United States.”67

With government funding now being provided to the statutes for anti-bullying programs in educational facilities, various states are taking the correct approach in proposing school safety acts that focus on adolescent bullying and harassment both on and off campus. Even if such state legislation becomes effective, the new laws do not evade constitutional review for free speech protections. Although the provisions may clearly show that home-based computer harassment of a fellow student or school figure can be deemed to fall within the scope of disciplinary action for cyber-bullying in school district policies, it is still necessary to prove sufficient connection between the speech and the school environment, and that the activities cause sufficient disruption to the educational forum.68 Regardless, instituting mandatory school district policies will at a minimum raise awareness of the problem of online harassment and put the students on notice that such activities are not acceptable and could very well result in harsh consequences. This, in itself, is a large step forward given that students, parents, and educators are now armed with the knowledge that the problem, in fact, can be addressed.

**Protections for Today**

Victimizing using electronic media is an increasing trend with dangerous consequences. News broadcasts of adolescent suicide, school bullying, and gun violence have become commonplace—a disturbing societal reality. It is only recently that we have begun to hear disturbing news of yet another shooting in a school environment and far too many deaths. We hear repeated news stories of isolated adolescents using the Internet to broadcast their violent messages. While there is no defined profile for these violent offenders and no clear link to cyber-bullying at this time, it would not be surprising to learn that such a connection did exist. For the educators, there is a fine line between the protection of student free speech and the liabilities for not taking action when there is the knowledge of the act of cyber-bullying. As public policy, protection of our youth requires us to err on the side of their protection. Curbing the speech of an adolescent is a small price to pay compared to the terror and torment suffered by victims and the long-term effects caused by the acts of cyber-bullies.

Even though Congress is making steps to address the problem of school violence, states are attempting to implement statutes that include prohibition of online bullying, and school districts are initiating policies including disciplinary actions against cyber-bullies, the biggest defense at present is parental protection. Parents need to be more involved in the online activities of their children, know where they “surf,” and how they communicate. Parents make conscious efforts to protect their children from sexual predators and shield them from online obscenity, but should also give adequate recognition to the dangers of the newest online aggressor: the cyber-bully. Education and awareness are paramount, both for the student bully and the victim. Recognizing the signs of both may be the preventative weapon to save children from years of online tormenting as suffered by Jeffrey Johnston in Florida. The “school yard” environment has always been the arena for adolescent cruelty towards each other;
however, the online forum provides a new, stronger weapon that leaves the victim in a position that even away from school, there is no escape.

There are numerous websites and programs with ample information regarding cyber-bullying that are available for educators, parents, and students. While we patiently wait for the laws to effectively control cyber-bullying, while carefully balancing the First Amendment rights of students, this information should be utilized to its fullest. Counseling, support services, research and statistical studies, etc., are all available resources to help shield the youth of today from online bullies. Further, the awareness these information services provide can educate the offenders that such actions are not innocent fun, are far from harmless, can lead to devastating consequences, and do not go unnoticed and unpunished.

The problem of adolescent cyber-bullying is far from resolved. If anything, we are only becoming aware of the activities and its effects. While legislation and school policy are headed in the right direction, the problem is complex. With the protection of this country’s youth at stake, the attention of Congress and our courts needs to have enhanced focus on the continuously emerging threat of the cyber-bully.

Endnotes

3 Id.
10 Id.
11 U.S.Const. amend. I.
13 Staley v. Jones, 239 F.3d 769, 784 (6th Cir. 2001).
16 Id.
17 Id.
19 Id.
20 Id.
23 Id.
24 Id.
27 Id.
28 Id.
30 Id.
32 Id.
34 Id.
36 Id.
37 Id.
38 Id.
42 AOL.com, Terms of Use, http://about.aol.com/aolnetwork/aol-com_terms.
43 Id.
44 Lunney v. Prodigy Services Co., 94 N.Y.2d 242 (N.Y. 1999) (In Lunney, a “[m]inor sued Internet service provider (ISP) for defamation and negligence after imposter, who had
Recent Developments in Information Technology Law

By David R. Syrowik, Brooks Kushman, PC, Southfield, Michigan

U.S. Supreme Court

Patents

As reported at 74 BNA’s PTCJ 629 on September 25, 2007, the U.S. Supreme Court grants a writ of certiorari in a case appealing the Federal Circuit’s ruling that conditional sales of microprocessors and chipsets made by Intel Corp. pursuant to a license did not exhaust the combination patent rights of licensor LG Electronics Inc. As further reported at 75 BNA’s PTCJ 246, the petitioners, supported in amicus briefs by the government and others, argue that a patent owner is entitled to no more than one royalty on the sale of a patented article, that an authorized first sale of the patented article fully exhausts the patent owner’s rights in that article, and that the Federal Circuit’s conditional sales case law in the exhaustion context conflicts with Supreme Court precedent. Quanta Computer Inc. v. LG Electronics Inc.

U.S. Courts of Appeal

Patents

As reported at 74 BNA’s PTCJ 491, on August 20, 2007, the U.S. Court of Appeals for the Federal Circuit held in banc that proof of willful infringement permitting enhanced damages requires at least a showing of objective recklessness, and thus there is no longer an affirmative obligation that a patent infringement defendant obtain an opinion of competent legal advice before initiating possibly infringing activity. In so ruling, the court overturns its 1983 decision in Underwater Devices Inc. v. Seagate Technology LLC.

As reported at 74 BNA’s PTCJ 630, 679, on September 26, 2007, the U.S. Court of Appeals for the Federal Circuit, in a splintered ruling, largely affirms patent infringement judgments and injunctive relief against Vonage Holdings Corp. for infringing several Verizon Services Corp. patents on voice-over-Internet-protocol, or VoIP technology, but it vacates the controversial $58 million damages award and sends the case back to the lower court for a new trial. The appellate court’s much-anticipated ruling comes on the heels of a jury verdict against Vonage awarding $69.5 million in damages in a similar patent infringement dispute with Sprint Communications Co. As further reported at 75 BNA’s PTCJ 9, on October 25, 2007, Vonage announced that it has settled its patent infringement dispute about voice-over-Internet-protocol, or VoIP technology with Verizon. As still further reported at 75 BNA’s PTCJ 88, on November 15, 2007, the Federal Circuit refused Vonage’s petition for rehearing. Vonage says in a press statement that it has agreed to pay up to $120 million. Verizon Services Corp. v. Vonage Holdings Corp.
As reported at 74 BNA's PTCJ 631, on September 20, 2007, the U.S. Court of Appeals for the Federal Circuit held that signals that are embedded with information allowing them to place digital watermarks on electronic data files are unpatentable because they fit into none of the four categories of patentable subject matter set forth in Section 101 of the Patent Act. Affirming a ruling by the Board of Patent Appeals and Interferences rejecting patentability for certain claims, the court finds that the signals themselves are not patentable as a “process, machine, manufacture, or composition of matter.” The court rules that “some physical form for the signal is required,” and that the patent applicant’s claims represent merely “transitory embodiments . . . not directed to statutory subject matter.” In re Nuijten.

As reported at 75 BNA's PTCJ 214, on December 26, 2007, the U.S. Court of Appeals for the Federal Circuit held that an erroneous claim construction rendered partially invalid an award of summary judgment in favor of Google Inc. The court directed the lower court to reexamine whether Google's AutoLink data management software infringes two patents. Hyperphrase Technologies LLC v. Google Inc.

As reported at 74 BNA's PTCJ 635, on September 20, 2007, the U.S. Court of Appeals for the Federal Circuit held that patent claims directed to mental processes for resolving a legal dispute between two parties by the decision of a human arbitrator are abstract ideas unpatentable under Section 101 of the Patent Act. Affirming an unpatentability ruling, the court finds that most of the claims “seek to patent the use of human intelligence in and of itself.” In re Comiskey.

As reported at 83 USPQ2d 1264, on July 3, 2007, the U.S. Court of Appeals for the Federal Circuit held that accused device, which employs “reduced instruction set computer” microprocessor, does not meet “general purpose computer” limitation in claims of patent for interactive computer system for guiding emergency personnel in conducting CPR, since prosecution history created estoppel against reading “general purpose computer” to include dedicated microprocessor such as RISC. Hutchins v. Zoll Medical Corp.

As reported at 84 USPQ2d 1146, on August 24, 2007, the U.S. Court of Appeals for the Federal Circuit held that in view of disclosure in specification, claims for computer aided design and manufacture of custom orthodontic appliances, which require determination of finish positions of teeth, are properly construed to require automatic determination of finish positions, even though claims do not expressly recite such automatic control.Ormco Corp. v. Align Technology Inc.

As reported at 75 BNA's PTCJ 92, on November 16, 2007, the U.S. Court of Appeals for the Federal Circuit upheld a jury verdict that Microsoft Corp. infringed two patents for reducing software piracy because it is supported by substantial evidence. z4 Technologies Inc. v. Microsoft Corp.

As reported at 75 BNA's PTCJ 273, on January 8, 2008, the U.S. Court of Appeals for the Federal Circuit noted that issues of fact as to whether a prior art article on cyber security was sufficiently publicly accessible on a non-indexed FTP server preclude a summary judgment that this reference is a “printed publication” invalidating patents for anticipation under Section 102(b) of the Patent Act. Vacating and remanding the summary judgment of invalidity based on the Live Traffic prior art reference, the appellate court finds fact issues as to whether skilled artisans can locate the article by navigating the non-indexed and non-catalogued FTP server on which it was posted for seven days. SRI International Inc. v. Internet Security Systems Inc.

**Patents/Antitrust**

As reported at 84 USPQ2d 1129, on September 4, 2007, the U.S. Court of Appeals for the Third Circuit ruled that plaintiff has stated claim for monopolization in violation of Sherman Act's Section 2 based on allegation that defendant induced standards-determining organizations to include defendant’s patented technology in mobile wireless telephony industry standard by falsely promising to license technology on fair, reasonable, and nondiscriminatory terms. Broadcom Corp. v. Qualcomm Inc.

**Copyrights**

As reported at 75 BNA's PTCJ 291, on January 16, 2008, the U.S. Court of Appeals for the Sixth Circuit held that a plaintiff’s copyright claims against a licensor do not require arbitration if the claims can be addressed “without reference to” the scope of the parties’ underlying software arbitration agreement. Reversing the dismissal of those claims, the appellate court faults the lower court for applying an overly broad “touches upon” standard, rather than assessing whether the plaintiff’s infringement claims could be resolved “without reference to the software contract.” NCR Corp. v. Korala Associates Ltd.
As reported at 74 BNA’s PTCJ 267, on June 21, 2007, the U.S. Court of Appeals for the Eleventh Circuit held that an online database that substantially duplicated yacht information posted on a competitor’s multiple listing service infringed the original site’s compilation copyright on the selection and arrangement of that information. Affirming a lower court decision in favor of the plaintiff, the court says that the idea and expression had not merged to make the database uncopyrightable. **BUC International Corp. v. International Yacht Council Ltd.**

As reported at 74 BNA’s PTCJ 296, on July 3, 2007, the U.S. Court of Appeals for the Ninth Circuit held that credit card companies cannot be held liable for contributory or vicarious copyright infringement when their customers buy infringing images online. Affirming the dismissal of copyright and trademark claims, the court emphasizes that facilitating a payment is peripheral to the actual infringement, which is the unauthorized distribution of a copyrighted work. **Perfect 10 Inc. v. Visa International Service Association.**

As reported at 75 BNA’s PTCJ 277, on January 4, 2008, the U.S. Court of Appeals for the Fifth Circuit held that a defendant in a copyright infringement case—who was not the person using his Internet account to infringe musical works through Kazaa—was not entitled to recover legal expenses incurred up to the point that the correct defendant was identified and the claims dropped. **Virgin Records America Inc. v. Thompson.**

As reported at 85 USPQ2d 1217, on December 7, 2007, the U.S. Court of Appeals for the Second Circuit held a federal district court did not have jurisdiction to approve a settlement agreement between a class of freelance authors and a group of publishers that allegedly reproduced the authors’ work without their permission because the bulk of the works in question were unregistered and the Copyright Act of 1976 gives federal courts jurisdiction only over registered works. **In re Literary Works in Electronic Databases Copyright Litigation.**

As reported at 83 USPQ2d 1331, on June 26, 2007, the U.S. Court of Appeals for the Sixth Circuit held that defendant distributor of karaoke “compact disc plus graphics” packages containing plaintiffs’ copyrighted musical works and graphic displays of songs’ lyrics is not entitled to defense of fair use; defendant’s assertion that karaoke packages are used for educational purposes is without merit. **Zomba Enterprises Inc. v. Panorama Records Inc.**

As reported at 83 USPQ2d 1040, on June 14, 2007, the U.S. Court of Appeals for the Sixth Circuit held that terms of “dealer agreement” between parties warrant finding that infringement plaintiff is entitled to award of actual damages for infringing copies of computer software, made by defendant, that were not used by defendant’s customers. **Thoroughbred Software International Inc. v. Dice Corp.**

**Trademarks**

As reported at 74 BNA’s PTCJ 661, on September 26, 2007, the U.S. Court of Appeals for the Ninth Circuit held that there is no cause of action for trademark disparagement under the Lanham Act. Vacating an order enjoining the defendant from making disparaging comments and ordering him to take down disparaging statements already posted to the Internet, the appellate court also criticizes the trial court for concluding that the plaintiff had demonstrated a likelihood of success on the merits of its trademark infringement claim without applying the likelihood of confusion test. **Freecycle Network Inc. v. Oey.**

As reported at 75 BNA’s PTCJ 93, on November 5, 2007, the U.S. Court of Appeals for the Ninth Circuit held that online sale of “PerfumeBay” perfume infringes “eBay” mark. **Perfumebay.com Inc. v. eBay Inc.**

As reported at 75 BNA’s PTCJ 213, on December 28, 2007, the U.S. Court of Appeals for the Ninth Circuit held that a federal district court appropriately granted eBay Inc. summary judgment in a trademark infringement case against it. The court, however, agrees that eBay was not entitled to attorneys’ fees. **Applied Information Sciences Corp. v. eBay Inc.**

**Trade Secrets**

As reported at 74 BNA’s PTCJ 698, on September 17, 2007, the U.S. Court of Appeals for the Fifth Circuit held that software licenses that do not authorize the licensee to create derivative computer programs are not relevant to the question of when a trade secret misappropriation claim accrued with regard to the defendants’ use of a proprietary program to create a competing program. **General Universal Systems Inc. v. Hal Inc.**
Right of Publicity

As reported at 74 BNA's PTCJ 772, on October 16, 2007, the U.S. Court of Appeals for the Eighth Circuit held that a company that promotes Internet “fantasy baseball” games did not violate the ballplayers’ publicity rights. C.B.C. Distribution and Marketing Inc. v. Major League Baseball Advanced Media LP.

U.S. District Courts

Patents

As reported at 74 BNA's PTCJ 271, on June 15, 2007, the U.S. District Court for the Eastern District of Texas held that the balance of equities justify enjoining the infringer of an Australian research organization’s patent on wireless technology, despite the fact that the parties are not competitors. Granting the patent holder's motion for permanent injunction under the Supreme Court’s eBay test, the court also stresses that the public interest is advanced by encouraging the kind of research and development in future technologies that led to the plaintiff’s patent. Commonwealth Scientific and Industrial Research Organisation v. Buffalo Technology Inc.

As reported at 75 BNA's PTCJ 214, on December 10, 2007, the U.S. District Court for the Western District of Wisconsin held that two Internet billing patents requiring a trusted third party to provide customers with the “communications link” of Internet access are not infringed by eBay Inc. and PayPal Inc. Netcraft Corp. v. eBay Inc.

As reported at 74 BNA's PTCJ 401, on July 27, 2007, the U.S. District Court for the Eastern District of Virginia held that the four-part test for the issuance of permanent injunctions recently reaffirmed by the U.S. Supreme Court requires the denial of a motion for a permanent injunction against online auction operator eBay Inc. On remand from the high court, the trial court for the second time refuses to bar eBay's use of its familiar “Buy It Now” purchasing system, which had been adjudged to infringe patents on electronic commerce. MercExchange LLC v. eBay Inc.

As reported at 74 BNA's PTCJ 445, on August 6, 2007, the U.S. District Court for the Southern District of California voided a jury award of $1.5 billion in patent infringement damages against Microsoft Corp. While the court denies several of the software giant’s multiple challenges to the jury verdict, it stresses that the “net result” of its ruling is a judgment in Microsoft’s favor. Lucent Technologies Inc. v. Gateway Inc.

As reported at 74 BNA's PTCJ 447, on August 6, 2007, the U.S. District Court for the Southern District of California held that Qualcomm waived its rights to enforce certain patents related to digital video technology standards because it deliberately concealed information from a standards-setting body. As further reported at 75 BNA's PTCJ 255, on January 7, 2008, Qualcomm attorneys were sanctioned and ordered to pay Broadcom $8.5 million. Qualcomm Inc. v. Broadcom Corp.

As reported at 75 BNA's PTCJ 136, on November 27, 2007, the U.S. District Court for the Northern District of California held that the alleged infringement of a patent through aggregation of data from multiple commercial Web sites by a Pakistan-based operation is not reachable as making, using, or selling the invention under 35 U.S.C. § 271(a). Granting a summary judgment of noninfringement on that basis, the court, however, did not dismiss a claim under 35 U.S.C. § 271(g) for importing a product made by a patented process. CNET Networks Inc. v. Etilize Inc.

As reported at 75 BNA's PTCJ 60, on November 8, 2007, to resolve all claims pending between the parties in a lawsuit pending in the U.S. District Court for the Western District of Wisconsin, Vonage Holdings says that it has reached a settlement with AT&T Corp., making the third time in recent months that the struggling online telephone service has come to terms with major U.S. telephone companies charging it with patent infringement. As further reported at 75 BNA's PTCJ 282, the companies announced on December 21, 2007 that the settlement of the patent infringement action was finalized. AT&T Corp. v. Vonage Holdings Corp.

As reported at 74 BNA's PTCJ 692, on October 8, 2007, to resolve all claims pending between the parties in a lawsuit pending in the U.S. District Court for the District of Kansas, Sprint Communications Co. and Vonage Holdings Inc. announce that they have settled their ongoing patent infringement dispute and entered into a licensing arrangement under Sprint’s voice-over-packet, or VOP patent portfolio. Sprint Communications Co. v. Vonage Holdings Corp.
Copyrights

As reported at 83 USPQ2d 1910, on August 14, 2007, the U.S. District Court for the Western District of Texas held that plaintiff is denied summary judgment that “Mirage” computer animation software at issue is joint work that plaintiff is entitled to distribute independently despite termination of distributorship agreement between parties, since provisions of agreement referring to “TVPaint Software and Technology” can be interpreted as identifying defendant as originator and owner of software, and since those provisions, and affidavit testimony submitted by defendants, raise fact questions about ownership of “Mirage” animation software, and about whether plaintiff’s contributions were merged into inseparable and interdependent parts of software. Bauhaus Software Inc. v. TVPaint Development.

As reported at 75 BNA’s PTCJ 165, on November 29, 2007, the U.S. District Court for the Southern District of New York denied an injunction because plaintiff failed to demonstrate substantial similarity between Web sites. Bio-Safe One Inc. v. Hawks.

As reported at 84 USPQ2d 1174, on August 29, 2007, the U.S. District Court for the District of Idaho held that defendant was employee of plaintiff corporation, rather than independent contractor, and the source code that defendant worked on while employed by plaintiff is, therefore, owned by plaintiff as work made for hire, since plaintiff provided defendant with tools and instrumentalities, since defendant was hired for indefinite amount of time and for various duties, rather than for single discrete project to be completed in specific amount of time, and since defendant was paid salary, not lump sum at completion of job. JustMed Inc. v. Bye.

As reported at 84 USPQ2d 1640, on September 12, 2007, the U.S. District Court for the Eastern District of Pennsylvania held that infringement defendants are denied summary judgment that plaintiff is claiming copyright protection for uncopyrightable system, concept, or idea, since plaintiff has presented evidence that defendants copied or slightly altered written content from plaintiff’s Web sites and then presented that content on defendants’ Web sites, and since plaintiff’s claims are not based on alleged infringement of marketing system or concept per se. ConsulNet Computing Inc. v. Moore.

As reported at 83 USPQ2d 1741, on May 21, 2007, the U.S. District Court for the Northern District of California held that claim for common law misappropriation, in which plaintiff operator of social networking Web site alleges that competing site collected e-mail addresses of users of plaintiff’s site and used those addresses to solicit users’ patronage, is not preempted by federal copyright law, since data that defendant allegedly misappropriated is not subject to copyright protection per se, and since defendant has not shown that it is alleged to have misappropriated uncopyrightable work of authorship. Facebook Inc. v. ConnectU LLC.

As reported at 75 BNA’s PTCJ 63, on November 6, 2007, the U.S. District Court for the Middle District of Georgia held that whether a 13 or 14-year old defendant who admittedly violated the Copyright Act by downloading and distributing music on the Internet is entitled to reduced statutory damages as an innocent infringer is a question of fact entitling the defendant to a jury trial. Electra Entertainment Group Inc. v. McDowell.

As reported at 83 USPQ2d 1584, on July 17, 2007, the U.S. District Court for the Eastern District of Virginia held that plaintiff’s registration of copyright for computer software is invalid, and district court therefore lacks subject matter jurisdiction over plaintiff’s infringement claim, since no original copies of source code for software remain, and plaintiff was able to produce “copy” for deposit only by referring to modified versions of code and redacting those modifications to best of his recollection in order to create “original” copy. Tavory v. NTP Inc.

As reported at 74 BNA’s PTCJ 779, on October 16, 2007, the U.S. District Court for the Central District of California entered a permanent injunction requiring filtering against final Grokster defendant. Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd.

As reported at 85 USPQ2d 1297, on November 30, 2007, the U.S. District Court for the Eastern District of New York struck the defense of copyright misuse on ground of legal insufficiency in action in which record companies claim that defendant illegally downloaded and shared copyrighted music using file-sharing Web site, since defendant alleges that plaintiffs have engaged in copyright “pooling,” but defendant has not alleged that plaintiffs pooled their copyrights for mutual benefit, or that they abused their combined market power to detriment of copyright consumer. UMG Recordings Inc. v. Lindor.

As reported at 74 BNA’s PTCJ 410, on July 19, 2007, the U.S. District Court for the District of Oregon held that a city was not liable for constitutional violations under 42 U.S.C. § 1983 when one of its employees disconnected a modem hosting offensive Web site material. American Buddha v. City of Ashland.
As reported at 74 BNA's PTCJ 495, on August 10, 2007, the U.S. District Court for the District of Utah held that Novell Inc. did not transfer the copyrights in the UNIX operating system as part of a development deal and is entitled to summary judgment on a claim asserting that it made false public statements of copyright ownership. *SCO Group Inc. v. Novell Inc.*

As reported at 74 BNA's PTCJ 694, on October 4, 2007, a jury in the U.S. District Court for the District of Minnesota found a defendant who shared digital versions of 24 music recordings online liable for copyright infringement and it awards $222,000 to the plaintiff record companies. *Virgin Records America Inc. v. Thomas.*

As reported at 75 BNA's PTCJ 252, in plaintiff's brief filed December 7, 2007 in the U.S. District Court for the District of Arizona, plaintiff stated that evidence that a defendant in a copyright infringement case saved digitized music files uploaded from compact discs in a folder that will allow them to be shared over Kazaa is sufficient to prove unauthorized distribution of the copyrighted works. *Atlantic Recording Corp. v. Howell.*

As reported at 84 USPQ2d 1551, on September 28, 2007, the U.S. District Court for the Eastern District of New York held that digital geographic base map files that display images of tax blocks and tax lots in New York City are sufficiently original to qualify for copyright protection, since, in creating predecessor database to map files, city planning department programmers made numerous decisions concerning number and location of coordinates used to depict various shapes in maps, and concerning which features to incorporate and which to exclude. *New York v. GeoData Plus LLC.*

As reported at 75 BNA's PTCJ 168, on November 20, 2007, the U.S. District Court for the Southern District of California held that a Web site featuring unoriginal features, fonts were eligible for copyright only as collection. *Allen v. Ghoulish Gallery.*

As reported at 85 USPQ2d 1154, on December 7, 2007, the U.S. District Court for the Western District of Michigan issued subpoenas to record companies for students at Michigan State University. The court specified that the university and the targets of the lawsuit should have an opportunity to move to quash or modify the subpoenas. *Arista Records LLC v. Doe.*

As reported at 85 USPQ2d 1018, on October 16, 2007, the U.S. District Court for the Central District of California held that plaintiff is likely to demonstrate that defendant infringed plaintiff's copyrights by accessing and using Web site, on which plaintiff sells tickets for entertainment and sports events, in violation of site’s “terms of use,” since terms of use create nonexclusive license to view, and thus copy, pages from site, and use of work in violation of license gives rise to liability for infringement, and since plaintiff is highly likely to prove that devices marketed by defendant for accessing and navigating plaintiff’s site are prohibited “automated devices” that interfere with proper working of site, and that violate license provisions limiting frequency of ticket purchase requests. *Ticketmaster LLC v. RMG Technologies Inc.*

As reported at 85 USPQ2d 1157, on December 7, 2007, the U.S. District Court for District of Columbia held that record companies seeking to identify alleged infringers had shown good case for a subpoena directing Georgetown University to identify students who used the computers targeted in the lawsuit. The court ruled that compliance with the subpoena would not violate the university’s obligations under federal law to protect the personal information of the students. *Warner Bros. Records Inc. v. Doe.*

**Copyrights/DMCA**

As reported at 74 BNA's PTCJ 270, on June 20, 2007, the U.S. District Court for the Central District of California held that the extent to which YouTube has the right and ability to control allegedly infringing content posted on its video-sharing Web site is a question of fact that cannot be disposed of at the summary judgment stage. *Tur d/b/a Los Angeles News Service v. YouTube Inc.*

As reported at 74 BNA's PTCJ 374, on July 21, 2007, the U.S. District Court for the Eastern District of Pennsylvania held that a law firm that looked at past versions of a Web site on the publicly accessible Internet Archive did not circumvent access controls in violation of the Digital Millennium Copyright Act when the malfunctioning archive allowed access to pages that the owner had wanted restricted. Granting a defendant's motion for summary judgment, the court emphasizes that the access was the result of errors on the part of the archive's server. *Healthcare Advocates Inc. v. Harding, Early, Follmer & Frailey.*
Trade Secrets

As reported at 74 BNA’s PTCJ 385, on June 27, 2007, the U.S. District Court for the Northern District of California held that theft of trade secrets will irreparably harm wireless developer and, consequently, a former employee and his new company were temporarily enjoined. *Posdata Co. v. Kim.*

Trademarks

As reported at 75 BNA’s PTCJ 41, on October 24, 2007, the U.S. District Court for the Northern District of Texas ruled that an infringement lawsuit challenging Google Inc.’s use of American Airline Inc.’s marks in advertising may go forward. *American Airlines Inc. v. Google Inc.*

As reported at 75 BNA’s PTCJ 280, on January 2, 2008, the U.S. District Court for the Western District of Washington held that a musical group that used the term “Wailers” as part of its band name and domain name did not engage in cybersquatting. *Ormsby v. Barrett.*

As reported at 75 BNA’s PTCJ 280, on December 5, 2007, the U.S. District Court for the District of Massachusetts held that purchase of competitor’s mark as search keyword is trademark “use” in commerce. *Boston Duck Tours v. Super Duck Tours.*

As reported at 75 BNA’s PTCJ 281, on December 27, 2007, the U.S. District Court for the District of Nevada held that adding “e” before trademark in domain named deemed evidence of actual trademark dilution. *Visa International Service Association v. JSL Corp.*

International Trade Commission

Patents

As reported at 74 BNA’s PTCJ 446, on August 6, 2007, U.S. Trade Representative Susan Schwab decides to allow the International Trade Commission’s orders to become final in its investigation involving Qualcomm Inc. mobile phones. *In re Certain Baseband Processor Chips and Chipsets, Transmitter and Receiver (Radio) Chips, Power Control Chips, and Products Containing Same, Including Cellular Telephone Handsets.*

U.S. Patent and Trademark Office

Trademarks

As reported at 74 BNA’s PTCJ 482, on July 31, 2007, following the *Dell* and *Lands’ End* cases, the TTAB finds Web site printouts acceptable evidence of use. *In re Valenite Inc.*

As reported at 83 USPQ2d 1220, on February 21, 2007, the TTAB held that copy of Web page submitted by applicant as specimen of use is not display used in association with goods sufficient to support registration of “CondomToy condom” as trademark for condoms, since prospective customers reading Web page are likely to view proposed mark as descriptive or informational term, or as advertising puffery, and since Web page is simply advertisement for condoms, and does not function as point-of-purchase display. *In re Osterberg.*

As reported at 83 USPQ2d 1444, on April 17, 2007, the TTAB held that proposed “Lens” mark is generic for applicant’s “retail store services featuring contact eyewear products rendered via a global computer network,” since, in view of finding that “lens” is shorthand name for contact eyewear that is subject of applicant’s services, term is also generic name for retail Internet store services themselves. *In re Lens.com Inc.*

As reported at 83 USPQ2d 1351, on February 21, 2007, the TTAB held that goods offered in connection with applicant’s “Inquest” mark must be considered closely related to opposer’s goods for purposes of likelihood-of-confusion analysis, since applicant’s goods, described in application as “computer software for use by institutions and individuals . . . to conduct research . . . and to automate reports,” represents large slice of broad array of goods actually offered by opposer under “ProQuest” mark and trade name, as well as goods covered by opposer’s federal registrations for “ProQuest” mark. *ProQuest Information and Learning Co. v. Island.*
As reported at 84 USPQ2d 1028, on June 18, 2007, the TTAB held that Internet evidence is generally admissible and may be considered for purposes of evaluating trademark, with respect to evidence taken from Wikipedia. However, the TTAB will only consider such evidence if non-offering party has opportunity to rebut that evidence by submitting other evidence that may call accuracy of proffered Wikipedia information into question. In re IP Carrier Consulting Group.

As reported at 84 USPQ2d 1560, on July 31, 2007, the TTAB held that a petition for cancellation of respondent’s registration for “ABS-CBN” trademark for satellite and cable television broadcasting services and telephone calling-card services is barred by laches and acquiescence, since respondent has pleaded and proved those equitable defenses, and since it is not “inevitable” that confusion will arise from respondent’s broadcasting services and those offered by petitioner under its “CBN” mark, in that parties’ marks are not identical, and have been in concurrent use for 13 years without any reported instances of actual confusion. Christian Broadcasting Network Inc. v. ABS-CBN International.

As reported at 75 BNA’s PTCJ 137, on November 21, 2007, the TTAB held that the fame of the “Spam” mark for canned meat cannot be extended to prevent use of the term for unsolicited e-mail. Hormel Foods Corp. v. Spam Arrest LLC.

As reported at 85 USPQ2d 1285, on March 15, 2007, the Trademark Trial and Appeal Board held that the examining attorney has established prima facie case that applicant’s proposed “Watson” mark, for computer software used in laboratory information management, is primarily merely surname, since “Watson” is not rare surname, and evidence supports finding that “Watson” has “look and feel” of surname; applicant has failed to rebut prima facie case by arguing that proposed mark qualifies for registration as historical name or geographical term. In re Thermo LabSystems Inc.

**State Laws and Decisions**

**New Mexico**

As reported at 74 BNA’s PTCJ 412, on June 13, 2007, the New Mexico Supreme Court held that as the copyright owner, a Web designer, not the person who hired the designer, is owner of Web site. New Mexico v. Kirby.

**Wisconsin**

As reported at 83 USPQ2d 1085, on May 15, 2007, the Wisconsin Supreme Court held that school district’s public disclosure of compact disc and memorandum containing adult images and Internet searches that plaintiff public school teacher allegedly viewed and conducted on his school computer is fair use of copyrighted materials in memo and on CD; allowing public access to CD and memo for purposes of adhering to Wisconsin's Open Records Law will not affect potential marketability of copyrighted materials. Zellner v. Cedarburg School District.

**Illinois**

As reported at 85 USPQ2d 1129, on August 2, 2007, the Illinois Appeals Court held that plaintiff’s claims under Illinois Right of Publicity Act, based on defendant’s use of plaintiff’s images on Internet in business of licensing copyrights for photographs and other artistic images, are not preempted by federal copyright law under 17 U.S.C. § 301. Brown v. ACMI Pop Division.

You can find back issues of this newsletter at [http://www.michbar.org/computer/newsletters.cfm](http://www.michbar.org/computer/newsletters.cfm)
Technology Outsourcing: Move It Now or Fix It First?

By Mark G. Malven, Dykema

Which is the better option: fix a technology function before shipping it out for outsourcing, or ship it out first? This is sometimes known as the “fix or ship” question. There is no universal right answer. This is an issue that requires case-by-case analysis. Fixing existing operations means improving the organization’s efficiency and effectiveness. In general, the “fix” can range from a minor process to a major functional design that changes core business functions.

Questions to Consider

The first key question an organization considering outsourcing should contemplate is whether it understands the dysfunctional process that it proposes to outsource. If an organization does not understand its own “mess,” then it will not be able to determine what the best practices are for that function, nor will it know whether a potential supplier is providing the best practices.

Because each situation requires its own analysis, the organization’s decision will depend not only on the type of change needed but also on the assessment of the business drivers and constraints. The following factors will be helpful in arriving at a decision:

- organizational impact
- urgency and criticality
- change complexity
- potential impact on scope/service levels
- cost and effort for implementation
- outsourcing feasibility with status quo
- provider delivery capability
- disruption to ongoing programs.

There are several other questions organizations should consider when contemplating whether to fix or outsource first:

- How does the price of fixing the dysfunctional process in-house compare to outsourcing it in its unstable state?
- Is the organization’s culture likely to produce an in-house fix?
- Is there adequate knowledge of the process to know what to ask and expect from a supplier?

The best option may be to receive a custom assessment before deciding which approach is the best for your organization.

Pros and Cons

So should an organization “fix it” or “move it”? There are several benefits associated with each approach.

**Benefits of Fixing First, then Moving.** The benefits of fixing a function before moving to outsource include (1) reducing the risk in transition to the service provider; (2) stronger capability to re-estimate the effort and scope of outsourcing required, as well as the potential improved service levels; (3) early realization of the perks from the change implementation/reengineering; and (4) service provider resources may still be leveraged. The organization may also end up with a better process by outsourcing the right components, rather than outsourcing the entire department, thus getting a better return on investment.

**Benefits of Moving First, then Fixing.** The benefits of outsourcing the dysfunctional process from the start include (1) an early start of outsourcing benefits; (2) higher capability to leverage reasonably low-cost resources for the fix; (3) the ability to utilize the expertise of the service provider; (4) applying the savings from outsourcing to finance improvement programs; and (5) the chance to develop an in depth relationship with the service provider.

Another benefit of outsourcing at the outset is that the organization can avoid expending time and money to reengineer the in-house system. Some may feel that there is a mess for a reason and that the organization may not be able to fix it itself. In addition, outsourcing may be the fastest and most successful remedy. Outsourcers are not necessarily better managers than
in-house managers, but they are agents of change, and sometimes change is exactly what an organization needs.

Practical Contract Considerations

It is important to remember that by choosing to outsource a function, the organization is entrusting a part of its business to an outside party. Therefore, outsourcing always involves the acceptance of some level of risk by the customer. To mitigate these risks, be sure to ask questions such as (1) Does the supplier have the perseverance and commitment to be successful? (2) Does the supplier recognize what the organization needs? (3) Is the supplier competent to address emergency situations?

Remember, when organizations outsource a process that is presently dysfunctional, there will still be significant pressure on the supplier to do the job correctly immediately upon transition or shortly thereafter. Therefore, while the contract must be tightly drawn to serve the organization’s needs and mitigate its risks, it is possible to go too far in placing unrealistic demands on the vendor. This can backfire on the customer—vendors that realize they are in a bad deal (for them) will do what they can to reduce their costs in ways a customer may not like.

Finally, an organization thinking of outsourcing must consider not only its goals but also the transition time of outsourcing, the money involved (apparent and unknown), and the impact on the organization and its employees. It is also critical to get your professional advisors involved early in the process so you can maximize your ability to make a decision that is right for your organization.

About the Author

Leader of Dykema’s Technology Transactions Practice, Mark G. Malven has many years of experience structuring and negotiating high stakes technology transactions, with a particular focus on information technology, biotechnology and life sciences, entertainment, and manufacturing. He has handled hundreds of strategic technology transactions involving development, consulting, sponsored university research, manufacturing, licensing, distribution, value-added reseller, private-label, content licensing, e-commerce, acquisition, and joint venture relationships. Mr. Malven was one of the primary negotiators for two of the largest IT outsourcing transactions ever undertaken, involving billions of dollars in services. Also a licensed patent attorney, he was recognized as a Michigan SuperLawyer by the publishers of “Law & Politics.” He can be reached at (248) 203-0517 or mmalven@dykema.com.

Upcoming Events

September 17, 2008

The IT Law Section’s annual meeting takes place on Wednesday, September 17th, from 2 to 4 p.m. The day will begin with a business meeting, which will include the election of the officers and new council members. A program entitled “The Practice of Information Technology Law,” which is an overview of the different aspects of practicing information technology law will follow. The speakers will discuss their individual practices and specific areas of IT Law upon which their practices touch. More details about the meeting and speakers can be found at http://www.michbar.org/news/releases/archives08/AM/schedules.html.

October 29, 2008

The IT Law Section will also be sponsoring jointly with ICLE a 1/2 day program, entitled “Information Technology Law: What Every Lawyer Should Know.” The seminar will take place on October 29, 2008. Attendees can expect to learn about how to avoid overlooked problems in web site privacy policies and terms of use, how to maintain and protect domain names on the web, how to draft outsourcing agreements, how to analyze and negotiate software licenses, how to create enforceable e-contract for your clients, and how to safeguard your clients’ intellectual property interests on the web. Details of the seminar, registration information, and bio information for the presenters can be found at http://www.icle.org/seminars/seminar_schedule.cfm?PRODUCT_CODE=2008CI7712.