



STATE BAR OF MICHIGAN

# Michigan IT Lawyer

A Publication of the State Bar of Michigan Information Technology Law Section

<http://www.michbar.org/computer>

Table of Contents  
January 2009 ■ Vol. 26, Issue 1

- Information Technology Law –  
What Every Lawyer Should Know ..... 3
- Protecting Your Client’s Web Traffic,  
Reputation & Intellectual Property in  
Cyberspace..... 4
- Recent Developments in Information  
Technology Law..... 7
- E-mail Privacy –Whether Court Order  
Disclosure of E-mail Content, per the Stored  
Communications Act, Violates the Fourth  
Amendment..... 12
- Meet a Section Member ..... 22
- Publicly Available Websites for IT Lawyers ..... 23
- 2009 Edward F. Langs Writing Award ..... 24

## Bits and Bytes from the Chair

By Christopher J. Falkowski, *Falkowski PLLC*

“There is no success without hardship.”  
- Sophocles (496-406 B.C.), Greek playwright

On behalf of the [IT Law Section](#), I wish you and your loved ones a joyous holiday season. Hopefully this time of year presents you with a well-deserved opportunity to take a true hiatus from your professional responsibilities, even if only for a couple of days. If there is one thing about lawyers that non-lawyers have a pretty accurate grasp of, it is that lawyers typically keep very hectic schedules and that lawyers struggle to find enough hours in the day to do all of the things that need to get done. We are often overbooked, which presents serious challenges to those who care about us. It is my hope that you are able to find the time this season to focus on the people who are most important in your life. Whatever the state of the economy or the prospects for the auto industry, we are all richer for the family and friends who are there for us in the good times as well as the bad. May this holiday season present you with joyous opportunities to strengthen and truly enjoy these important relationships.

I am happy to report that the section’s [IT law seminar](#) held on October 29<sup>th</sup> at [St. John’s](#) in Plymouth was a success. The event was well attended by a relatively diverse cross-section of attorneys. Comments from the attendees were overwhelmingly positive. Thanks to everyone who participated in the seminar, particularly those whose hard work facilitated its success. Special thanks are in order for [Kim Paulson](#) and to [Charles Bieneman](#). Kim was the section’s Chairperson for the 2007-2008 year, and it was Kim’s vision and insight that made the seminar possible. For his part, Charles graciously volunteered to head up the logistics of the seminar working closely with [ICLE](#) every step of the way. The [IT Law Section](#) looks forward to building upon that success and intends to make the seminar an annual event. We have already committed to hosting the

*Michigan IT Lawyer* is published every other month. If you have an article you would like considered for publication, send a copy to:

Brian A. Hall  
Traverse Legal, PLC  
810 Cottageview Drive  
Suite G-20  
Traverse City, Michigan 49684  
e-mail: [brianhall@traverselegal.com](mailto:brianhall@traverselegal.com)

Continued on next page





2008-2009

Information Technology Section Council

Chairperson ■ Christopher J. Falkowski  
Chairperson-elect ■ Jeremy D. Bisdorf  
Secretary ■ Mark G. Malven  
Treasurer ■ Charles A. Bieneman

COUNCIL MEMBERS

Charles A. Bieneman  
Jeremy D. Bisdorf  
Donald M. Crawford  
Christopher J. Falkowski  
Samuel Frederick  
Brian A. Hall  
Karl A. Hochkammer  
Matthew M. Jakubowski  
William J. Lamping, Jr.  
Mark G. Malven  
Ronald S. Nixon  
Vincent I. Polley  
Frederick E. Schuchman III  
Jerome M. Schwartz  
David R. Syrowik  
Anthony A. Targan  
John L. Tatum  
Mary Ann Wehr

Immediate Past Chair

Kimberly A. Paulson

Ex-Officio

Claudia V. Babiarz  
Thomas Costello, Jr.  
Kathy H. Damian  
Robert A. Feldman  
Sandra Jo Franklin  
Mitchell A. Goodkin  
William H. Horton  
Lawrence R. Jordan  
Charles P. Kaltenbach  
Michael S. Khoury  
J. Michael Kinney  
Edward F. Langs\*  
Thomas L. Lockhart  
Janet L. Neary  
Kimberly A. Paulson  
Paul J. Raine  
Jeffrey G. Raphelson  
Frederick E. Schuchman III  
Steven L. Schwartz  
Carol R. Shepard  
Anthony A. Targan  
Stephen L. Tupper

Commissioner Liaison

Robert K. Fergan

Newsletter Co-Editors

Brian A. Hall  
Michael Gallo

Bits and Bytes . . .

*Continued from page 1*

second annual seminar with ICLE in the last week of October 2009. When a specific date is finalized, we will let you know. The council for the section will be spending the early part of the year exploring various possibilities with respect to topics and speakers. If you have suggestions or comments, please feel free to e-mail them to me at [chris@falkowskipllc.com](mailto:chris@falkowskipllc.com).

2009 looks to be an exciting year for the section and we are constantly looking for ways to provide value to our members. The section's longstanding newsletter titled the *Michigan IT Lawyer* is being published more frequently thanks to the efforts of co-editors [Brian Hall](#) and Michael Gallo. I encourage anyone who is interested to submit articles for publication in the section newsletter. Please take the opportunity to share your legal analysis, practice tips, and other insights with the members of the section.

This past November marked the premier issue of the section's new [e-newsletter](#). The focus of this new publication is to keep members informed of section events and to provide interesting snippets of IT-related articles with links to the full articles. [Ron Nixon](#) and [Samuel Frederick](#) are serving as co-editors of this new publication.

If you are interested in becoming more involved in the section, please contact me at [chris@falkowskipllc.com](mailto:chris@falkowskipllc.com). The section welcomes your participation and there will be a diverse range of opportunities to contribute to the section in 2009. Committees such as Membership/Recruitment, Programming, Annual Meeting, and the Spring Luncheon/Networking Event can always benefit from increased participation, with more hands making for lighter work.

Have a happy new year. I look forward to seeing you in 2009. ■

**Chris Falkowski**  
Chairperson 2008-2009  
IT Law Section

Statement of Editorial Policy

The aim and purpose of the Information Technology Law Section of the State Bar of Michigan is to provide information relative to the field of information technology law and other information that the section believes to be of professional interest to the section members. Unless otherwise stated, the views and opinions expressed in the *Michigan Information Technology Lawyer* are not necessarily those of the Information Technology Section or the State Bar of Michigan.

# Information Technology Law – What Every Lawyer Should Know

By Anthony Targan, *ProQuest*

On Wednesday, October 29, 2008, the Institute of Continuing Legal Education (ICLE) presented the above-titled seminar sponsored by the Information Technology Law Section. The half-day event took place at the Inn at St. John's in Plymouth, an impressive setting that added to the grandeur of the proceedings. The seminar was well attended, including 78 registrants, plus additional webcast participants. Incoming Section chair Chris Falkowski and Jeff Kirkey of ICLE welcomed the audience and conducted an introductory real-time survey of audience members to assess their background, practice areas, and meeting preferences. Moderator Charles Bieneman of Rader, Fishman & Grauer adeptly handled the challenge of keeping the presenters on schedule, while leaving adequate time for questions.

The first speaker, Robert Gurwin of AOL, gave an entertaining overview of "Issues to Consider When Conducting Business Online." Mr. Gurwin focused on privacy policies and the thorny issues raised by end user generated content, particularly on social networking sites. He also addressed website terms of service (TOS), and weighed the pros and cons of passive TOS (posting a link at the bottom of the home page) versus active TOS (requiring click-through acceptance as a condition of service). He said that websites should reserve the right to make changes in TOS and put the burden on the user to monitor the updated version. However, he noted that material changes to how information is shared with third parties might require e-mail notification or highlighting the updated policy on your website. Mr. Gurwin also touched on the subject of domain names.

A panel discussion on "Outsourcing Agreements: Vendors and Purchasers Square Off" featured some interesting point counter-point among Beth Mier of Computer Sciences Corporation, Daniel John Sepanik of Visteon, Karl Hochkammer of Foley & Lardner, and Mark Malven of Dykema. The panel discussed the outsourcing process and the interaction among sourcing consultants and inside and outside counsel. There was consensus on the benefits of including a form contract with a request for proposals (RFP) as a means of weeding out difficult vendors and setting expectations for risk allocation. The panel agreed that selective inclusion of the RFP and RFP

responses was better than wholesale incorporation to avoid ambiguity. The panel also debated key issues such as: (1) the customer's right to withhold payment pending resolution of disputes; (2) the difficulty of developing metrics to measure service levels; and (3) the inevitability of "scope creep."

Another panel addressed "Software Licenses: Key issues for Business Lawyers." Panelists included Kathryn Ossian of Miller Canfield, Thomas Iacobelli of Compuware and Donald Crawford of Harman International Industries. The panel reviewed key legal terms in most software licenses, with particular emphasis on representations and warranties, limitations on liability, and indemnification provisions. Most panelists agreed that the indemnity is more important than the warranty, and that in cases of intellectual property infringement, the remedy to provide a non-infringing substitute is often more important than monetary damages. Limitations of liability are typically not hard caps and can include "carve-outs" for infringement, breaches of confidentiality, and compliance with laws.

Chris Falkowski of Falkowski PLLC presented "Offer and Acceptance in an Online World." In addition to discussing basic contract formation principles and electronic signatures, he spoke about the importance of being able to correct mistakes or make changes in automated online transactions—did the individual have the opportunity for "prevention or correction of the error"? Mr. Falkowski also discussed the perils of navigating the alphabet soup of conflicting laws such as E-Sign, UETA and UCITA.

The final presenter was Michael Stewart of Rader, Fishman & Grauer who tackled the broad topic of "IP on the Web." Mr. Stewart provided an overview of the basics of intellectual property law, including patents, trade secrets, trademarks, and copyrights. He did an excellent job of providing real world examples of how these rights—and rights holders—often conflict in the online environment. Some of his more entertaining examples included: (1) Amazon's efforts to protect its "one-click" patent; (2) Allegations of trade secret leaks by whistle-blower site Wikileaks.org; (3) Google's efforts to fight trademark "genericide"; (4) Free speech and fair

use implications of “ihate...” and “...sucks” domain names; and (5) Virtual reality property rights in online games.

Overall, the seminar was very well received. Moderator Charles Bieneman expressed his hope that this could become

an annual event. Special thanks were offered to the ICLE and to the three sponsoring law firms, Dykema, Foley & Lardner, and Rader, Fishman & Grauer. ■



## Protecting Your Client’s Web Traffic, Reputation & Intellectual Property in Cyberspace

By C. Enrico Schaefer, *Traverse Legal*

Most companies do not understand the extent to which their web traffic, reputation and intellectual property are under attack on the internet. Each day, companies lose control of their domain names to hackers, disgruntled partners and ex-employees who, with the click of their mouse, put their victims out of business on the web. Companies often don’t realize that their brands and trademarks are under attack from domain squatters who divert their web traffic, costing those companies customers and revenue.

Too often, companies fail to take even the most rudimentary steps to protect themselves online. While no company would purposely leave the front door of their business unlocked when they leave at night, these same companies essentially leave their on-line presence largely unprotected from on-line scammers, thieves and other threats.

Lawyers have a unique opportunity to help their clients understand the most common online threats and put measures in place to reduce their on-line risk. You don’t have to be an internet lawyer or understand software code in order to become an essential ingredient in your client’s online protection system. But you do need to understand the basics.

**Phishing Attacks:** Phishing attacks use trademark protected brands of reputable companies under false pretenses to obtain usernames, passwords, credit card numbers or other proprietary information from innocent third parties. These are the well disguised but bogus emails you receive in your inbox from eBay, PayPal, Bank of America and other companies which ask you to provide otherwise confidential

or private information. Oftentimes, the domain name is a typographical variant of the real company whose trademarks are being leveraged as part of fraud. Most people don’t recognize that the email, the hyperlink or the web site are a fraud until it is too late.

Phishing attacks obviously harm consumers, but think about the company whose trademarks are being leveraged to perpetrate the fraud. In 2007, an estimated \$3 billion dollars was lost by U.S. businesses as a result of their customers being subjected to phishing attacks.

What can you do for your client to protect against phishing? Educate your client and tell them to educate their staff to report any unusual consumer complaints. You can also use monitoring services such as PhishTank which is a community-based anti-phishing service at [www.phishtank.com](http://www.phishtank.com). There are experts available to track phishing emails upstream and phishing databases such as the Anti-Phishing Working Group [www.antiphishing.org](http://www.antiphishing.org). You can also work directly with ISPs, domain registrars and other entities in order to block phishing emails before it hits your customer’s inbox. Phishing is regulated by both civil and criminal anti-fraud laws. Some states have enacted anti-phishing laws to protect their state residents.

**Cybersquatting Attacks:** Cybersquatting is the act of registering, trafficking in, or using a domain name with the bad faith intent to profit from the trademark rights belonging to someone else. Essentially, cybersquatting is registering a domain name that is identical or similar to a trademark be-

longing to your client in order to confuse consumers into thinking that the web site is sponsored, endorsed or owned by the trademark holder. Typosquatting is a form of cybersquatting, where the squatter registers a typographical variation of your client's trademark knowing that a percentage of internet users will incorrectly type your client's brand into the browser address bar.

Cybersquatting and typosquatting is extremely common on the internet. High traffic web sites often have dozens or even hundreds of cybersquatters diverting their traffic. Many companies have no idea that their trademarks or domain names are being squatted. Even on low traffic web sites, direct competitors sometimes register similar domain names in order to directly divert customers looking for your client to their competing product or service.

Cybersquatting can cause serious problems for your client beyond the loss of web site traffic and revenue. Oftentimes, phishing and malware attacks occur through domain names similar to your client's trademark in order to confuse consumers. Further, federal courts have held that a failure to protect trademarks can result in a waiver of trademark rights. Therefore, allowing cybersquatters and typosquatters to exist can diminish your client's trademark rights, or extinguish them altogether.

There are a variety of tools on the internet designed in order to identify domain names which may violate your client's trademarks. [www.domaintools.com](http://www.domaintools.com) offers a typo search tool which will identify typographical variations of your client's domain names and identify the registrant of those domain names. Trademark monitoring services such as [www.marktend.com](http://www.marktend.com) will alert you if trademark registrations or domain names are registered using your client's trademarks. [www.domainfight.net](http://www.domainfight.net) can help you locate habitual cybersquatters.

If your client is the victim of a cybersquatter, you can pursue relief through the Uniform Domain Name Resolution Policy (UDRP) or the Anticybersquatting Consumer Protection Act (ACPA) of 1999. The UDRP is an arbitration policy put in place by the Internet Corporation for Assigned Names and Numbers (ICANN) which allows any trademark holder to file a complaint against any domain registrant who it believe is violating its trademarks. The UDRP is the only law in the history of the world which is truly global. It doesn't matter where the domain registrant is located; they are bound by the UDRP and subject to a domain transfer order from a UDRP arbitration panelist. The ACPA is a federal law amending the trademark violation provisions of the Lanham Act, which provides specific relief for trademark infringement related to domain names.

**Keyword Advertising:** The two major online advertising tools are Google Adwords and Yahoo's Overture system. Both companies offer pay-per-click (PPC) advertising placements on their search engine result pages and throughout their content networks of blogs and other web sites. Anyone can pay for an advertisement to show up through Adwords or Overture, and propagate that advertisement across the internet.

What happens if your client's competitors start bidding on your client's trademarks as part of their keyword advertising campaign? Depending on how the advertisement displays and the hyperlinked landing page content, the competitor may be infringing your client's trademarks. Similar to all other trademark issues, the consumer confusion test applies to this particular form of potential online trademark infringement. This is an emerging area of trademark law under the Lanham Act which has gained considerable attention in 2008. Both Google and Yahoo have developed polices for dealing with keyword infringement, which are available on each of their web sites. Trademark infringement threat letters often eliminate the unwanted behavior and the courts remain a viable option when the keyword infringement continues.

There are several monitoring tools such as [www.marktend.com](http://www.marktend.com) which will provide comprehensive reports concerning keyword use of your client's trademarks in both Google and Yahoo advertising campaigns. Your job as the attorney is to review the report information and determine which advertising keyword uses are likely to cause consumer confusion and follow up with a threat letter.

**Domain Name Theft:** A common complaint among domain name owners is that they have lost control of their domain name and thus their web site. Typically, domains are lost because the registrant information on file with the registrar is controlled by someone else. Oftentimes, a partner or co-owner will register the domain name under his or her own email address. The domain registrant's email address is the linchpin to control any domain name with the domain registrar (i.e. GoDaddy, Network Solutions, Moniker). Other companies allow their employees, often younger IT professionals, to register the domain names. When that employee leaves, the renewal notices go unanswered to a now non-existent email address and the domain registration expires. Other times, companies let their outsourced web developers register a domain name without specific parameters as to how the domain will be registered and who will be listed as the domain registrant. When a dispute arises between partners, with a disgruntled employee, or the web development company, the domain name becomes leverage. "I'll take down your web site" is a pretty sobering thing to hear from



someone who is no longer on your team. In some instances, the domain registrant login information is hacked, allowing a third party to take control of the domain name.

Many companies do hundreds of thousands or millions of dollars of business online, or rely on their web sites as part of their core business. Many of these same companies have no idea who is listed as the registrant of their key domain names.

The first step a lawyer should take is to work with the client to conduct an audit of all domain names and registrant information. Make sure that all domain registrant information is in the name of the company, the whois information is accurate and that the email listed on the registrant account is controlled by the client with email forwarding set up to multiple key executives for any changes in registrant information. Monitoring services such as [www.domaintools.com](http://www.domaintools.com) will send you an email if any changes occur in the registrant information on any domains input into the system. There are also companies that will control your client's portfolio of domain names for a small price in order to ensure that domains do not lapse and remain the property of the company. Move your domains to a registrar such as Moniker who has a strong record of protecting domain names from thieves and hackers. Moniker, for instance, has a premium program which will ensure that no changes in a domain names registrant information occurs without a telephone call to a pre-identified individual.

If your client loses control of their domain name, threat letters and litigation can sometimes regain control. The ACPA has a special in rem provision which allows certain federal courts to take control of a domain which has been stolen and transfer it back to its rightful owner. But these strategies take time. In the meantime, your client's web site will likely be lost. The best tactic is to ensure that there are no problems up front.

**Content Scraping & Copyright Violations:** Content scraping is the act of copying your client's content and pasting it onto third party web sites. Content scrapers essentially want to build traffic on their web site. The easiest way for them to develop those web sites is to steal content from other sites including text, images and video. This can do considerable damage to your company because search engines such as Google and Yahoo can penalize your client's search engine ranking based on duplicate text content. Moreover, your client's customers could easily get confused if they land on a web site with your client's scraped content which suggests common ownership, affiliation, or sponsorship. There are numerous tools on the internet which will monitor online plagiarism such as [www.copyscape.com](http://www.copyscape.com). Registering your client's

key content with the Copyright office is always a good idea. If your client has a registered copyright or can show original authorship, a Digital Millennium Copyright Act (DMCA) take-down notice to the infringing party or other online provider (i.e. Typepad, Blogger, Facebook, Twitter, etc.) should result in scrubbing of that content from the internet.

**Gripe Sites & On-Line Defamation:** Nothing is more shocking than typing your company or personal name into Google only to see a gripe site or defamatory content returned as a page 1 search result. If your client's customers are exposed to gripe site information, it could do serious damage to client relationships and revenue. If your executives are targeted by disgruntled employees or customers, their reputations could be the subject of a web site which could potentially be there forever. While the First Amendment to the United States Constitution protects most online commentary, it does not insulate authors and publishers from liability for defamation or unfair competition. Typically, threat letters to everyone involved in authoring and displaying the content online is a good first step in dealing with these situations. You should also check any service provider or web hosts' Terms of Service. Often times, web vendors specially preclude their customers from publishing defamatory content. If so, they may enforce the Terms of Service against the author/publisher of the content and take the site down. If the content is on a blog, forum or bulletin board, contact the service provider with specific information about the defamatory statements and demand that the content be immediately removed. In certain instances, you can have the gripe sites removed from the search engine database altogether, so that the search results don't linger long after the site has been removed from the web.

In conclusion, the internet poses a number of hazards to virtually every business, both big and small. Devising an online brand protection program is critical in order to head off problems before they occur. Every lawyer with business clients needs to understand the basic forms of attack, monitoring tools and strategies available for protecting his or her clients in the online world. ■

### About the Author

*Mr. Schaefer is the founding attorney of [TraverseLegal](http://TraverseLegal.com), a law firm dedicated to global on-line brand protection. He is a seasoned trial attorney practicing internet, domain and trademark law on a global basis. Mr. Schaefer is a frequent author and presenter on issues related to protecting business interests in a global internet economy.*

# Recent Developments in Information Technology Law

By David R. Syrowik, *Brooks Kushman P.C.*

## U.S. Courts of Appeal

### Patents

As reported at 77 BNA's PTCJ 4, on October 31, 2008, the U.S. Court of Appeals for the Federal Circuit, in an *en banc* splintered opinion, affirmed a decision by the Patent Office that a process directed to managing the consumption risk costs of a commodity is not patentable subject matter. The majority opinion concludes that the patent applicant's claims were ineligible for patent protection under 35 U.S.C. § 101 because they claimed a non-transformative process that encompassed purely mental steps without the aid of a computer or other device. *In re Bilski*.

As reported at 76 BNA's PTCJ 515, on August 1, 2008, the U.S. Court of Appeals for the Federal Circuit ruled that a district court committed clear error by ignoring whether information not disclosed to the Patent and Trademark Office was material and by finding inequitable conduct solely based on a patentee's lack of candor. The patents were directed to halftoning technology used in computers and printers. Reversing a ruling of unenforceability, the court takes the unusual step of having the case remanded to a different judge since statements and rulings by the judge below favoring Microsoft Corp. made bias an issue. *Research Corporation Technologies Inc. v. Microsoft Corp.*

As reported at 76 BNA's PTCJ 620, on August 29, 2008, the U.S. Court of Appeals for the Federal Circuit decided that Cygnus lost its appeal of judgments that the on-sale bar invalidated its "callback" technology patents and that its trade secret misappropriation claim is barred by the statute of limitations. Cygnus's failure to present evidence in the district court's summary judgment proceedings contribute to both decisions against the company. *In re Cygnus Telecommunications Technology LLC Patent Litigation*.

As reported at 76 BNA's PTCJ 733, on September 19, 2008, the U.S. Court of Appeals for the Federal Circuit affirmed in large part the ITC patent non-infringement ruling in favor of Qualcomm's accused chipsets. Communications networks compliant with "EV-DO" wireless communications standard developed and promoted by respondent in Tariff Act exclusion action do not necessarily infringe claims of patent that require telephone handset to be operable in power-saving "sleep state," since there is no evidence that handsets

operating under standard must power down their receivers in sleep state in order to be compatible with EV-DO networks, and since EV-DO standard does not require that handset even enter sleep state. *Broadcom Corp. v. International Trade Commission*.

As reported at 76 BNA's PTCJ 896, on October 14, 2008, the U.S. Court of Appeals for the Federal Circuit, in the latest installment of the long battle between wireless telecommunications rivals Broadcom Corp. and Qualcomm Inc., lifts the International Trade Commission's exclusion order against imported cell phones with Qualcomm chipsets, ruling that the agency used the wrong standard to determine whether the company induced customers to infringe Broadcom's patents. *Kyocera Wireless Corp. v. International Trade Commission*.

As reported at 76 BNA's PTCJ 759, on September 25, 2008, the U.S. Court of Appeals for the Federal Circuit affirmed a judgment relieving Microsoft Corp. from a jury award of over \$1.5 billion for infringement of Lucent Technologies Inc.'s patents. *Lucent Technologies Inc. v. Gateway Inc.*

As reported at 76 BNA's PTCJ 811, on September 24, 2008, the U.S. Court of Appeals for the Federal Circuit held that a jury verdict of liability for induced infringement that was based on whether defendant Qualcomm obtained a letter from opinion counsel need not be overturned in light of the *en banc* ruling in *In re Seagate*. Upholding the verdict of induced infringement, the court rejects the argument that *Seagate* altered the state of mind requirement for inducement and says that the *en banc* ruling in *DSU Medical Corp. v. JMS Co.* "remains the relevant authority" on inducement. *Broadcomm Corp. v. Qualcomm Inc.*

As reported at 76 BNA's PTCJ 864, on October 10, 2008, the U.S. Court of Appeals for the Federal Circuit, reviewing a district court's case for the third time, finally affirms a patent invalidity finding based on the "simple substitution" criterion for finding obviousness under the U.S. Supreme Court's *KSR* decision. Despite a jury finding of validity and infringement, the appellate court affirms the trial court's grant of a motion for judgment as a matter of law because a prior art patent disclosed all but a new technique – well known by the time of the patent application – for communications among computers in a manufacturing plant. *Asyst Technologies Inc. v. Emtrak Inc.*

As reported at 76 BNA's PTCJ 869, on October 9, 2008, the U.S. Court of Appeals for the Federal Circuit ruled that a district court's "flawed" reading of amendments to claims in a reexamined patent led it to incorrectly conclude that a software patent is invalid for asserting improper claim scope. *Predicate Logic Inc. v. Distributive Software Inc.*

### Copyrights

As reported at 76 BNA's PTCJ 584, on August 13, 2008, the U.S. Court of Appeals for the Federal Circuit ruled that the holder of a copyright in a computer program for model trains made available for free public download may enforce an "open source" copyright license to control future use and distribution of that work by downstream users. Vacating a ruling that denied the copyright owner a preliminary injunction, the appellate court finds that the terms of the "Artistic License" on the plaintiff's Web site are enforceable as conditions that govern a downloader's right to modify and distribute the copyrighted work, not merely covenants to be enforced under contract law. *Jacobsen v. Katzer.*

As reported at 76 BNA's PTCJ 511, on August 4, 2008, the U.S. Court of Appeals for the Second Circuit reversed a lower court finding and holds that a cable television service offering digital video recording of television and movie programming at central sites – rather than on a home set-top box – is not a direct infringement of the copyright in those programs since "copies" were not created within the meaning of the Copyright Act. *Cartoon Network LP v. CSC Holdings Inc.*

As reported at 76 BNA's PTCJ 519, on July 31, 2008, the U.S. Court of Appeals for the Sixth Circuit held that the government's failure to show how a defendant's importation of counterfeit DVDs and labels is "contrary to law" made an indictment defective, but the defect is harmless error. *United States v. Teh.*

As reported at 76 BNA's PTCJ 698, on September 9, 2008, the U.S. Court of Appeals for the Ninth Circuit held that a contractor who created and installed several software programs for a customer, and was paid a substantial fee for his services, impliedly granted the customer an unlimited license to use, modify, and retain the source code in the programs. The court rules that the company did not infringe the contractor's copyright by continuing to use the software after the contractor was fired. *Asset Marketing Systems Inc. v. Gagnon.*

As reported at 76 BNA's PTCJ 701, on September

12, 2008, the U.S. Court of Appeals for the Eleventh Circuit held that a federal court may not exercise subject matter jurisdiction over an action for a declaration that a customer of a software development company retains the right to use and modify custom software without infringing the developer's copyright, when the software was never registered with the Copyright Office. *Stuart Weitzman LLC v. Microcomputer Resources Inc.*

### Copyrights /DMCA

As reported at 87 USPQ2d 1667, on August 4, 2008, the U.S. Court of Appeals for the First Circuit ruled that the district court properly granted summary judgment to plaintiff cable television service provider on claim that defendants violated Digital Millennium Copyright Act by selling low-frequency signal filters, within plaintiff's service area, that were capable of bypassing plaintiff's pay-per-view billing mechanism, since plaintiff's pay-per-view delivery and billing system is a technological measure that effectively controls access to copyrighted works, and digital cable filter allows subscribers to "avoid" or "bypass" that technological measure. *CoxCom Inc. v. Chaffee.*

### Trademarks

As reported at 88 USPQ2d 1051, on August 28, 2008, the U.S. Court of Appeals for the First Circuit affirmed summary judgment of infringement in action in which defendants admitted that they incorporated plaintiff's works in metatags and invisible text on their Web site, for express purpose of attracting customers to site. *Venture Tape Corp. v. McGills Glass Warehouse.*

As reported at 76 BNA's PTCJ 911, on October 10, 2008, the U.S. Court of Appeals for the Eleventh Circuit ruled that a mark's use on Web site available in Florida sufficed to establish personal jurisdiction there. *Licciardello v. Lovelady.*

## U.S. District Courts

### Patents

As reported at 77 BNA's PTCJ 17, on October 29, 2008, the U.S. District Court for the Central District of California ruled, in a case of first impression, that Qualcomm Inc. is entitled to the return of \$11 million in "sunset" royalties it paid pursuant to a permanent injunction since the injunction was reversed after the wireless network patent at issue was found invalid by the Federal Circuit on appeal. *Broadcom Corp. v. Qualcomm Inc.*



As reported at 77 BNA's PTCJ 19, on October 24, 2008, the U.S. District Court for the Southern District of Florida ruled that a bulk e-mail distribution patent was invalid as non-statutory subject matter under 35 U.S.C. § 101 in part because it merely applied the concept "if at first you don't succeed, try, try again" to the abstract idea of fulfilling an order. *Perfect Web Technologies Inc. v. InfoUSA Inc.*

### Copyrights

As reported at 88 USPQ2d 1260, on June 10, 2008, the U.S. District Court for the Central District of California ruled that language on promotional CDs released by plaintiff record company to music industry "insiders," which states that "[t]his CD is the property of the record company and is licensed to the intended recipient for personal use only. Acceptance of this CD shall constitute an agreement to comply with the terms of the license. Resale or transfer of possession is not allowed and may be punishable under federal and state laws," does not create license, and defendant, who obtained promo CDs from record stores and online sources and resold them in online auctions, is protected by first sale doctrine. *UMG Recordings Inc. v. Augusto.*

As reported at 76 BNA's PTCJ 629, on August 15, 2008, the Associated Press and VeriSign Inc. settled litigation in the U.S. District Court for the Southern District of New York, alleging VeriSign subsidiary, Moreover Technologies Inc., misappropriated AP content online. The terms of the settlement were confidential. *Associated Press v. Moreover Technologies Inc.*

As reported at 87 USPQ2d 1730, on July 25, 2008, the U.S. District Court for the Northern District of California held that purpose and character of defendants' use, amount and substantiality of portion of work used, and effect of use on potential market for work warrant finding of fair use in action in which plaintiff, host of nationally syndicated radio program, claims that defendant American-Islamic organizations infringed plaintiff's copyright in program by posting four-minute audio clip on their Web site. *Savage v. Council on American-Islamic Relations Inc.*

As reported at 76 BNA's PTCJ 740, on September 19, 2008, a judge in the U.S. District Court for Eastern District of Virginia set 18-month music piracy jail term for a man who owned and operated a computer server; the convicted computer owner was also fined \$2,500. *United States v. Gitarts.*

As reported at 87 USPQ2d 1762, on June 9, 2008, the U.S. District Court for the Northern District of California granted plaintiff partial summary judgment of liability on its copyright infringement claim, since plaintiff has submitted sufficient evidence to show access and copying, including evidence that managing director of defendant company received copy of software shortly before defendant was incorporated, that defendant's software is nearly identical to plaintiff's work, and that defendant developed accused software with unusual speed in view of its small size, and defendant has failed to directly address any of this evidence. *Tableau Software Inc. v. Any Aspect KFT.*

As reported at 76 BNA's PTCJ 920, on October 28, 2008, in a pair of lawsuits pending in the U.S. District Court for the Southern District of New York, the Authors Guild, the Association of American Publishers, and Google Inc. announced that they have agreed to settle lawsuits in which the copyright holders alleged that Google's Book Search project infringed their copyrights. Under the terms of the settlement, Google will pay a total of \$125 million to establish a centralized royalty collection organization, to compensate authors of scanned books, and to pay the plaintiffs' legal fees. *Authors Guild v. Google Inc. and McGraw-Hill Cos. v. Google Inc.*

As reported at 87 USPQ2d 1880, on July 1, 2008, the U.S. District Court for the Western District of Pennsylvania granted defendants' motions to dismiss plaintiff's copyright infringement claims without prejudice, since complaint alleges that defendants have infringed plaintiff's copyrighted software for computerized system for repair and maintenance of electrical systems, but complaint does not identify whether single copyright registration protects software as whole, or whether multiple registrations protect individual components of software, and since plaintiff has failed to allege what conduct by defendant has infringed each of respective copyrights. *Tegg Corp. v. Beckstrom Electric Co.*

### Copyrights/DMCA

As reported at 76 BNA's PTCJ 626, on August 20, 2008, the U.S. District Court for the Northern District of California held that the "good faith belief" standard for issuing a takedown notice under the Digital Millennium Copyright Act requires copyright holders to consider whether the use of a copyrighted work falls within fair use exceptions to the Copyright

Act. In a matter of first impression, the court holds that, though an extensive investigation is not required, a copyright holder must have a subjective belief that a use of a copyrighted work is infringing and does not fall within fair use exceptions in order to issue a DMCA takedown notice in good faith. *Lenz v. Universal Music Corp.*

As reported at 76 BNA's PTCJ 672, on August 27, 2008, the U.S. District Court for the Northern District of California held that format conversion of user-submitted videos does not create liability for online service since the service took measures to fall within the safe harbor provisions of the DMCA. *lo Group Inc. v. Veh Networks Inc.*

### **Trademarks**

As reported at 76 BNA's PTCJ 658, on August 25, 2008, the U.S. District Court for the Northern District of California barred an online ticket company suspected of conning customers out of promised tickets to the 2008 Beijing Olympic Games from using the Olympic's marks. *U.S. Olympic Committee v. Xclusive Leisure and Hospitality Ltd.*

### **Antitrust**

As reported at 87 USPQ2d 1859, on February 2, 2008, the U.S. District Court for the Northern District of California held that an electrical engineer is qualified to testify, in antitrust action, regarding dynamic random access memory industry's perception of defendant's interface technology, and industry's knowledge of possibility that defendant might obtain patents reading on standards set by Joint Electron Devices Engineering Counsel. *Hynix Semiconductor Inc. v. Rambus Inc.*

### **Trade Secrets**

As reported at 87 USPQ2d 1756, on April 23, 2008, the U.S. District Court for the Western District of Pennsylvania held that the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, which punishes unauthorized access to stored electronic communications except in particular enumerated circumstances, does not preempt claims for violation of Pennsylvania's Uniform Trade Secrets Act asserted against defendants who allegedly used and disclosed contents of e-mail messages containing proprietary information that were inadvertently sent to defendants' servers; disclosure provisions of SCA clearly do not apply to defendants' conduct. *Ideal Aerosmith Inc. v. Acutronic USA Inc.*

### **Right of Publicity**

As reported at 88 USPQ2d 1243, on August 19, 2008, the U.S. District Court for the Eastern District of Michigan ruled that members of rock band did not state claim, under

Michigan law, for violation of their right of publicity against makers of video game, which features rerecorded version of one of band's songs synchronized into game, even though law protects against unauthorized use of name or likeness, since Michigan law does not recognize analogous claim based on sound of voice, let alone allegedly distinctive sound of combination of voices. *Romantics v. Activision Publishing Inc.*

## **U.S. Patent and Trademark Office**

### **Patents**

As reported at 87 USPQ2d 1826, on June 2, 2008, the Board of Patent Appeals and Interferences held in an unpublished opinion that claims directed to simulation systems using distributed computer network are patentable, even though claimed "simulating" is performed by solving purely mathematical representations of physical systems, without receiving information from real-world physical system or outputting data that controls real-world physical system, since claims are directed to particular machine implementation of mathematical algorithm that does not encompass every substantial practical application of abstract idea. *Ex parte Wasynczuk.*

### **Trademarks**

As reported at 76 BNA's PTCJ 595, on August 12, 2008, the Patent and Trademark Office withdrew its earlier preliminary approval of Dell Inc's intent-to-use application to register "Cloud Computing" as a trademark. *In re Dell.*

As reported at 87 USPQ2d 1623, on June 4, 2008, the Trademark Trial and Appeal Board ruled that the mark "Liquidadvantage," as shown in specimen of record consisting of page from brochure, does not function as service mark to indicate source of applicant's "custom manufacturing of pharmaceuticals featuring liquid fill and finish technology" services, since term "Liquidadvantage" in specimen clearly refers to proprietary software by that name, but specimen nowhere shows direct association between use of proposed mark and services for which registration is sought. *In re DSM Pharmaceuticals Inc.*

As reported at 87 USPQ2d 1953, on July 15, 2008, the Trademark Trial and Appeal Board dismissed an opposition to registration of "LifeZone" mark for educational services on ground of likelihood of confusion, since opposer failed to submit admissible evidence of its trademark registrations, and failed to provide evidence of common law trademark rights by showing prior use of its mark, since existence of opposer's Web site does not establish that opposer is using its mark on goods or services shown on Web site, and since opposer's recitation of prior use in pending application

does not constitute evidence of opposer's use or priority. *Life Zone Inc. v. Middleman Group Inc.*

As reported at 88 USPQ2d 1285, on September 29, 2008, the Trademark Trial and Appeal Board granted judgment on pleadings on issue of priority, since petitioner alleges, in its verified petition to cancel, that its pleaded "Clasificadosonline.com" and "Clasificados Online" marks were first used in

commerce on November 27, 1999, and since it is undisputed that respondent filed application that matured into its registration for "El Clasificado Online" mark on November 4, 1999, and Lanham Act provides that respondent may rely on this filing date as its constructive date of first use. *Media Online Inc. v. El Clasificado Inc.* ■



## E-mail Privacy –Whether Court Order Disclosure of E-mail Content, per the Stored Communications Act, Violates the Fourth Amendment

By Michael Gallo, EDS

### Introduction

"In 1997, the Department of Commerce reported that more e-mail was sent than regular mail[, and a]mong businesses, electronic mail has overtaken the telephone."<sup>1</sup> "[E]-mail privacy rights . . . derive their primary authority from the Electronic Communications Privacy Act (ECPA) . . . and the Fourth Amendment to the Constitution which specifically prohibits unreasonable searches and seizures."<sup>2</sup> "Given the importance of Internet communications and e-mail, it is very surprising how little caselaw exists addressing how the Fourth Amendment applies to it."<sup>3</sup>

The question is "whether e-mail users maintain a reasonable expectation of privacy."<sup>4</sup> The answer resides in understanding that "the underlying command of the Fourth Amendment is always that searches and seizures be reasonable. The determination of the standard of reasonableness governing any specific class of searches requires balancing the need to search against the invasion which the search entails."<sup>5</sup>

"Much debate has focused on the institutional competence [of Congress and the courts] to ensure that law keeps pace with technology. . . . Another approach understands technologists to be capable of regulating the capacity of their wares, [as well as being] capable of evading regulation."<sup>6</sup> "Legislators and judges must protect our most basic and fundamental personal freedom[s] even though . . . technologies present a serious challenge to law enforcement. To maintain a proper

balance between the needs of society and citizens' civil liberties, the American legal system must constantly react to emerging technologies."<sup>7</sup> ECPA passed in 1986, and lawmakers recognized that "the law must advance with the technology to ensure the continued vitality of the fourth amendment."<sup>8</sup>

This comment reviews the issue of email privacy, and whether disclosure of email information, pursuant to a court order authorized by the Stored Communications Act, violates the Fourth Amendment. The comment begins with an overview of sections of the Stored Communications Act that are critical to understanding the steps the government must take to compel Internet Service Providers to disclose email customer information. Next, the comment reviews efforts by the courts and commentators to balance the requirements of the Stored Communications Act and the constitutional requirements of the Fourth Amendment, using email disclosure analysis from *Warshak v. U.S.*<sup>9</sup> The comment concludes by considering whether *Warshak's* email disclosure analysis is correct, and by providing email disclosure predictions.

### Understanding the Stored Communications Act

"ECPA regulates how the government can obtain stored account information from network service providers such as ISPs. Whenever agents or prosecutors seek stored e-mail, account records, or subscriber information from a network service provider, they must comply with ECPA."<sup>10</sup> "The stored communication portion of [ECPA], 18 U.S.C. §§ 2701-2712,

creates statutory privacy rights for customers and subscribers of computer network service providers.”<sup>11</sup> These statutory privacy rights, known as the Stored Communications Act (SCA) create a set of Fourth Amendment like protections for wire or electronic communications while the communications are in electronic storage.<sup>12</sup>

While neither the SCA nor ECPA provide a suppression remedy for statutory violations, punishment for an offense under the SCA can be a fine, imprisonment, or both.<sup>13</sup> Willful violation of ECPA can lead to a suit against the government under 18 U.S.C. § 2712, in which the court can grant payment of actual damages, or \$10,000, whichever is greater, and reasonable litigation costs. If a constitutional violation is identified, constitutional remedies, such as suppression of evidence in a criminal case, may be appropriate, but a suppression remedy does not exist for non-constitutional violations.

#### Overview of § 2703 – Required Disclosure of Customer Communications or Records

“18 U.S.C. § 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail) and other information such as account records and basic subscriber information.”<sup>14</sup> Section 2703 offers the government three means<sup>15</sup> to compel providers to disclose information: a subpoena,<sup>16</sup> a § 2703(d) court order, and a search warrant.<sup>17</sup>

One feature of the compelled disclosure provisions of ECPA is that greater process generally includes access to information that can be obtained with lesser process. Thus, a § 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a § 2703(d) order can compel (and then some). As a result, the additional work required to satisfy a higher threshold will often be justified, both because it can authorize a broader disclosure and because pursuing a higher threshold provides extra insurance that the process complies fully with the statute. Note, however, the notice requirement must be considered as a separate burden under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using a § 2703(d) order without subscriber notice.<sup>18</sup>

Of particular interest is the § 2703(d) court order, with which law enforcement investigators can obtain wired or

electronic communication *content* information that has been in electronic storage for *more than 180 days* by showing “specific and articulable facts showing that there are reasonable grounds to believe that the contents”<sup>19</sup> to be seized “are relevant and material to an ongoing criminal investigation,”<sup>20</sup> As indicated within § 2703, there are instances in which the email account holder need not be given notice of the § 2703(d) court order or provided with an opportunity for judicial review of the request.

In comparison, to obtain wired or electronic communication *content* information that has been in electronic storage for *180 days or less*, law enforcement investigators must acquire a search warrant, which requires a finding of probable cause.

#### Terminology within the Stored Communications Act

To analyze and understand the SCA, familiarity with some terms is necessary: *content*, *electronic communication*, *electronic communication service*, *remote computing service*, and *electronic communications system*.

“‘**Contents**’, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.”<sup>21</sup> “Contents can be further divided into three subcategories: contents stored ‘in electronic storage’ by providers of electronic communication service; contents stored by providers of remote computing services; and contents held by neither.”<sup>22</sup>

“‘**Electronic Communication**’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include: (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in [18 USCS § 3117]); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.”<sup>23</sup>

ECPA differentiates between providers of *electronic communication service*, and providers of *remote computing service* using an *electronic communications system*. A specific service from a provider could be an electronic communication service, a remote computing service, or neither, with information stored in relation to each service possibly being regulated differently.

An **electronic communication service** (ECS) is “any service which provides to users thereof the ability to send



or receive wire or electronic communications."<sup>24</sup> "[T]he key issue in determining whether a company provides ECS is that company's role in providing the ability to send or receive the precise communication at issue, regardless of the company's primary business."<sup>25</sup>

A **remote computing service (RCS)** is defined as the "provision to the public of computer storage or processing services by means of an electronic communications system."<sup>26</sup> An **electronic communications system** is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."<sup>27</sup> "In contrast with a provider of ECS, a provider of RCS does not hold customer files on their way to a third intended destination; instead, [the files] are stored or processed by the provider for the convenience of the account holder."<sup>28</sup>

#### *Classifications and Disclosure Requirements under § 2703*

Classification of a system as being ECS, RCS, or neither is important, because disclosure of a message stored by RCS is regulated by § 2703(b), disclosure of a message stored by an ECS might be regulated by § 2703(a) or § 2703(b), and disclosure of a message stored by a system that is neither an ECS nor an RCS is not regulated by the SCA or ECPA, although disclosure would still be controlled by the Fourth Amendment.

Similar to the differentiation between ECS and RCS, ECPA treats 'electronic storage' and a 'remotely stored file' in different ways.

**Electronic storage** is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,"<sup>29</sup> or in the alternative as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."<sup>30</sup> "To determine whether a communication is in 'electronic storage,' it helps to identify the communication's final destination. A copy of a communication is in 'electronic storage' only if it is a copy of a communication created at an intermediate point that is designed to be sent on to its final destination."<sup>31</sup> "At that stage, the copy of the stored communication exists only as a temporary and intermediate measure, pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the e-mail, however, the communication reaches its final destination."<sup>32</sup>

Regrettably, the SCA does not provide a definition for a remotely stored file. The Department of Justice contends that "[i]f a recipient then chooses to retain a copy of the accessed communication on the provider's system, the copy stored on the network is no longer in 'electronic storage' because the retained copy is no longer in 'temporary, intermediate storage . . . incidental to . . . electronic transmission,' . . . and 'because the process of transmission to the intended recipient has been completed, the copy is simply a remotely stored file.'"<sup>33</sup> This contention is based on the interpretation that "the backup provision may refer to backups made by the provider for the provider's purposes."<sup>34</sup> Several district courts<sup>35</sup> agreed with this interpretation and have found that opened email messages *were not in electronic storage*.<sup>36</sup>

In opposition to the Department of Justice's contention is the interpretation that "the backup provision may refer to copies stored by the user for the user's purposes."<sup>37</sup> This interpretation was followed by the only federal appellate court to have addressed the issue, which determined that opened email messages *were in electronic storage*.<sup>38</sup> In supporting the view that user access converts an 'unopened message' to a 'message stored for the purpose of backup protection', the Ninth Circuit court determined that "[t]here is no dispute that messages remaining on [an ISP's] server after delivery are stored 'by an electronic communication service' within the meaning of 18 U.S.C. § 2510(17)(B),"<sup>39</sup> and that the "obvious purpose for storing messages on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again."<sup>40</sup>

The Ninth Circuit's analysis may be unpersuasive as a statutory interpretation, because "[t]he structure and history of the SCA suggest[s] that the backup provision of the definition of electronic storage exists to ensure that the government cannot make an end-run around [§] 2703(a)."<sup>41</sup> On the other hand, the Ninth Circuit's decision is consistent with the Sixth Circuit's vacated decision in *Warshak v. U.S.*,<sup>42</sup> which held that contents of email held by an ISP were protected by the Fourth Amendment.<sup>43</sup>

Compelled disclosure of a remotely stored file, *regardless of age*, is possible through a warrant, an administrative subpoena or a § 2703(d) court order.<sup>44</sup> To determine whether electronic storage is controlled by § 2703(a) or § 2703(b), one must know the *age of the email*. Pursuant to § 2703(a), compelled disclosure of email in electronic storage *for less than 181 days* must be by a warrant, while pursuant to § 2703(b), compelled disclosure of email in an electronic storage *greater than 180 days* can be by a warrant,<sup>45</sup> an



administrative subpoena,<sup>46</sup> or a § 2703(d) court order.<sup>47</sup> “The change in protection after 180 days presumably was intended to deal with abandoned e-mail, for which there presumably would be no reasonable expectation of privacy.”<sup>48</sup> “Of course, the use of e-mail has changed dramatically since the 180-day rule was created. Today a great deal of e-mail may sit on a remote server for more than 180 days without being abandoned.”<sup>49</sup>

#### *Requirements for a § 2703(d) Court Order*

Section 2703(d) defines the requirements for issuing a court order for disclosure of the contents of electronic communications in a remote computing service, and in certain instances, contents of electronic communications in electronic storage.<sup>50</sup>

For a § 2703(d) court order to be issued, the government must offer specific and articulable facts<sup>51</sup> showing reasonable grounds to believe the contents of the email to be seized are relevant and material to an ongoing criminal investigation.<sup>52</sup>

“Section 2703(d) imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not [as high as] a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against ‘fishing expeditions’ by law enforcement.”<sup>53</sup>

As defined in § 2703(b), the government must provide *prior notice* to the subscriber or customer to use a § 2703(d) court order to compel a provider to disclose the contents of electronic communications, **unless delayed notice is approved pursuant to § 2705.**<sup>54</sup>

Section 2705(a) allows the government to delay subscriber or customer notification for up to 90 days, if notification would have an adverse result, such as endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise jeopardizing an investigation or unduly delaying a trial. In addition, § 2705(a)(4) allows the court to grant extension of the delay of notification, upon application or by certification of government. “Upon expiration of the delayed notice period, [§ 2705(a)(5)] requires the government to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber.”<sup>55</sup>

#### *Government Procedures for Applying the Stored Communications Act*

Governmental entities must apply ECPA classifications to

the case facts to determine the appropriate procedures for obtaining information. First, the type of service provided must be classified.<sup>56</sup> Second, the information sought must be classified.<sup>57</sup> Third, the government must determine whether to compel disclosure, or to accept voluntarily disclosed information. If seeking to compel disclosure, the means to compel must be selected.<sup>58</sup> If seeking to accept voluntarily disclosed information, the government must determine whether the statute allows voluntary disclosure of the type of information sought.<sup>59</sup>

To meet the statutory requirements of the SCA, and to satisfy constitutional requirements of the Fourth Amendment when compelling disclosure of email content, the government can secure a warrant, or can provide the subscriber or customer with prior notice. On the other hand, attempting to compel a provider to disclose contents of electronic communications through a § 2703(d) court order, without providing the subscriber or customer with prior notice, may satisfy statutory requirements of the SCA, but may lead to a Fourth Amendment challenge based on an expectation of email privacy.<sup>60</sup>

#### **Balancing the Fourth Amendment and the Stored Communications Act**

“Because there is a ‘strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is ‘reasonable,’ ‘[o]bviously the Court should be reluctant to decide that a search thus authorized by Congress was unreasonable and that the Act was therefore unconstitutional.’”<sup>61</sup> An important case that interpreted the SCA in relation to Fourth Amendment protections, *Warshak v. U.S.* considered whether a preliminary injunction was properly issued to prohibit the government from seizing “the contents of any personal email account maintained by an Internet Service Provider (‘ISP’) in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard.”<sup>62</sup>

#### *Factual and Procedural Background of Warshak v. U.S.*

In *Warshak*, the government was investigating mail and wire fraud, money laundering, and other federal offenses in connection with a company owned by Warshak.<sup>63</sup> Upon a finding of “specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation,”<sup>64</sup> the government obtained two virtually identical § 2703(d) court orders compelling two ISPs to turn over both content and non-content<sup>65</sup> information regard-

ing any accounts related to Warshak or associated parties.<sup>66</sup>

The court orders requested “[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) . . . and [c]ommunications not in ‘electronic storage’ which include any e-mail communications received by the specified accounts that the owner or user of the accounts has already accessed, viewed, or downloaded.”<sup>67</sup> Curiously, although the court orders include the first half of the definition of electronic storage related to *accessed information*, as listed in § 2510(17)(A), the court orders were deafeningly silent regarding the second half of the definition of electronic storage, related to purposes of *backup protection*, as listed in § 2510(17)(B).

The magistrate also found that prior notice of the court order to parties would seriously jeopardize the investigation, and approved delay of notice to Warshak.<sup>68</sup> Over a year after the first court order was received, Warshak was notified of the § 2703(d) court orders.<sup>69</sup> Warshak sought the government’s assurance that additional § 2703(d) court orders would not be sought, but the government would not provide such assurance.<sup>70</sup> In response, Warshak filed a request for a preliminary injunction, asking the court to enjoin the government from further use of the SCA to compel Warshak’s email content, unless using a search warrant as allowed by § 2703(a).<sup>71</sup> At issue was whether the government violated the Fourth Amendment and parts of the SCA by compelling ISPs to produce certain email “pursuant to warrantless search orders issued under the authority of SCA Section 2703(d).”<sup>72</sup>

In ruling on the motion for preliminary injunction, the district court determined that “18 U.S.C. subsections §§ 2703(b)(1)(B)(ii), 2703(d) and 2705 violate the Fourth Amendment . . . to the extent they collectively authorize the *ex parte* issuance of search and seizure orders without a warrant and on less than a showing of probable cause.”<sup>73</sup> On appeal, as a case of first review, a three judge panel for the Sixth Circuit affirmed the decision with a slight modification to the preliminary injunction,<sup>74</sup> becoming “the first federal appeals court to rule that e-mail users have a reasonable expectation of privacy regarding messages they send and store . . . finding important flaws in the federal statute that details procedures for the government to access stored electronic information in criminal investigations.”<sup>75</sup>

Four month later, at the request of the government, a majority of Sixth Circuit judges voted to rehear *Warshak* en banc, and ordered the earlier decision vacated.<sup>76</sup> “The government’s petition for rehearing *en banc* raised two procedural issues . . . : (1) whether Warshak had standing to seek to enjoin the government’s future use of *ex parte* §2703(d)

orders, and (2) whether the panel applied the proper standard in facially invalidating portions of the SCA.”<sup>77</sup> In a nine to five decision, the en banc court vacated “the preliminary injunction because Warshak’s constitutional claim [wa]s not ripe for judicial resolution”<sup>78</sup> and “remand[ed] the case to district court to dismiss Warshak’s constitutional claim.”<sup>79</sup>

#### Email Disclosure Arguments in *Warshak v. U.S.*

The core of the *Warshak*’s email disclosure analysis regards the merits of the claim of a Fourth Amendment violation.<sup>80</sup> Both Warshak and the government agreed that a § 2703(d) court order’s threshold of *specific and articulable facts that information sought is relevant and material to an ongoing criminal investigation*, is a lesser standard than probable cause.<sup>81</sup>

#### Closed Container

Warshak asserted that a lesser standard violated the “Fourth Amendment presumption that ‘closed packages and containers may not be searched without a warrant’ issued upon a showing of probable cause.”<sup>82</sup> “To the extent the Act allows the government to compel disclosure of private e-mail communications without a warrant, it violates well-established Supreme Court ‘closed container’ jurisprudence.”<sup>83</sup> “As long as a package is ‘closed against inspection,’ the Fourth Amendment protects its contents ‘wherever they may be,’ and the police must obtain a warrant to search it just ‘as is required when papers are subjected to search in one’s own household.’”<sup>84</sup>

Warshak compared contents of a personal email account held by an ECS to the contents of a **sealed package** held by a third party carrier, and argued that while the government may seize such items to prevent loss or destruction, the Fourth Amendment requires a warrant be obtained in order to examine the contents.<sup>85</sup> The government compared a personal email account to a **postcard**, and argued for a warrantless inspection because the contents are visible at any time to the provider, who reserves the right to access email contents for various necessary purposes.<sup>86</sup>

The district court analyzed the opposing viewpoints by considering whether a subscriber has a *reasonable expectation of privacy* when email is stored by a provider.<sup>87</sup> In deciding for Warshak, the court was not persuaded that providers regularly access subscriber email in a Fourth Amendment sense, and that email screening, as for viruses or child pornography, does not affect a subscriber’s expectation that providers do not read regularly read subscriber email.<sup>88</sup> Although the appellate court’s vacated decision agreed with the district court’s reasoning that email stored by a provider “were roughly analogous to sealed letters, in which the

sender maintains an expectation of privacy,"<sup>89</sup> the en banc court refused to "speculate as to the sort of accounts and privacy terms that different users may have,"<sup>90</sup> and chose "to 'await an as-applied challenge' to decide whether the [SCA] is constitutional."<sup>91</sup>

#### Reasonable Relevance

The government joined two theories to create an argument for a reasonable relevance standard. The first theory was that a § 2703(d) court order is not a search, but is comparable to a third party administrative subpoena that compels disclosure under a reasonable relevance standard.<sup>92</sup> "When the government does not actually conduct the search for evidence, but instead merely obtains a court order that requires the recipient of the order to turn over evidence to the government within a specified period of time, the order complies with the Fourth Amendment so long as it is not overbroad, seeks relevant information, and is served in a legal manner."<sup>93</sup>

The second theory was that an email subscriber that voluntarily disclosed records to a third party maintained no expectation of privacy.<sup>94</sup> "Account holders may not retain a 'reasonable expectation of privacy' in information sent to network providers because sending the information to the providers may constitute a disclosure."<sup>95</sup>

Together, the 'administrative subpoena' and 'disclosure to a third party' theories formed the government's argument for a reasonable relevance standard. Because the contents of a subscriber's email were disclosed to a provider, the § 2703(d) court order compelled the provider to disclose information in which there was no expectation of privacy.<sup>96</sup> The appellate court's vacated decision ruled that although the theories were relevant, the argument "failed to pass muster"<sup>97</sup> by relying on the assumption the subscriber had no expectation of privacy.<sup>98</sup>

"The contents of e-mails are only 'exposed' in the limited sense that all information sent over a network is exposed to other machines."<sup>99</sup> By identifying whom email contents are shared with, or shielded from, a subscriber's expectation of email privacy can be determined.<sup>100</sup> Comparing an email provider to a telephone service provider, the court found that merely because a provider *could* access communication content, privacy expectation "is not diminished, because there is a societal expectation that the [provider] will not do so as a matter of course."<sup>101</sup> "The [vendor's] role as an intermediary was critical [to the finding,] . . . because the distinction between intermediary and destination are the crux"<sup>102</sup> of finding communication content has a heightened level of protection.<sup>103</sup>

The appellate court's vacated decision agreed with the district court that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP."<sup>104</sup> In contrast, the en banc court (which reviewed the case as a *facial* challenge to the Fourth Amendment, and not as an *as-applied* challenge) reflected that "expectations of privacy that computer users have in their e-mails . . . may well shift over time [and] from internet-service agreement to internet-service agreement"<sup>105</sup>, and recommended deciding "the validity of the [SCA] in the context of a specific internet-service agreement and a specific search and seizure."<sup>106</sup>

#### Unresolved Arguments: Privacy Expectations, Particularity, Stored Communications Act Classifications, and Protecting Expectations

One unanswered "question is how far such a principle can extend."<sup>107</sup> Although postal letters and telephone communications are both ordinarily protected by the Fourth Amendment, there are important exceptions.<sup>108</sup> Privacy expectations may fail for various reasons, such as terms of service that eliminate a subscriber's expectation of privacy, an individual who signs up for an account under fall pretense, or that content was stored without approval by a hacker.<sup>109</sup> An example of a failed email privacy expectation regards a Texas court that "ordered the City of Dallas to release e-mails from personal e-mail accounts and personally owned BlackBerries. The court held that the e-mails were subject to disclosure under the Texas Public Information Act because they were used by . . . officials to conduct public business."<sup>110</sup>

As pointed out by the vacated appellate court decision in *Warshak*, because the court found a general expectation of privacy, *Warshak* did not decide various alternate challenges, such as particularity.<sup>111</sup> Even if there is no general expectation of privacy, to prevent "wide-ranging rummaging searches,"<sup>112</sup> the particularity requirement of the Fourth Amendment may "necessitate that the scope of the search somehow be designed to target e-mails that could reasonably be believed to have some connection to the alleged crime being investigated."<sup>113</sup> "[W]here a subpoena or an SCA order compels the disclosure of e-mails, the demand must be reasonable in scope and relevance. . . . In either instance, a district court should consider whether the search could be narrowed by parameters such as the sender, recipient, date, relevant attachments, or keywords"<sup>114</sup>

The *Warshak* decision "suggests that the government can search through the e-mails it obtains after providing notice and serving a valid subpoena without obtaining probable

cause."<sup>115</sup> At least one observer believes "the opinion goes out of its way to reach many questionable . . . positions."<sup>116</sup> If the provider copied the email content on a computer disk, and if searching a computer disk is analogized to be "more like opening [unopened] mail than looking through already-opened papers,"<sup>117</sup> there are several precedents<sup>118</sup> suggesting that Fourth Amendment rules apply, and that a showing of probable cause may be appropriate.<sup>119</sup>

Regarding the merits of a Fourth Amendment claim, the *Warshak* courts did "not distinguish between messages read and unread by the subscriber, between messages newer or older than 180 days, or between originals and backup electronic copies"<sup>120</sup> Consideration of *age of the message*, or whether the message has been *accessed by the subscriber*, or whether the message is classified as *electronic storage* or a *remotely stored file*, could impact the constitutionality of delaying notice of the § 2703(d) court order pursuant to § 2705. "How these categories apply in practice is a surprisingly difficult question,"<sup>121</sup> because most of ECPA was passed in 1986, but "[t]echnology has changed, and the 1986 rules have not been updated to reflect those changes."<sup>122</sup>

An argument in support of the government, which was not considered by the court, is whether the subscriber's expectation of email privacy is one that society is willing to protect. Federal law has a "twofold requirement, first that a person have exhibited an [actual] subjective expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"<sup>123</sup> The government could advocate that the statute's allowance for delaying notice is evidence that the legislature determined that society does not recognize an expectation of email privacy as reasonable when there are specific and articulable facts that email contents are relevant and material to an ongoing criminal investigation. "The structure of ECPA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in stored e-mails than in subscriber account information."<sup>124</sup>

### Whether email disclosure analysis within *Warshak v. U.S.* is Correct

As stated at the beginning of this comment, the question is "whether e-mail users maintain a reasonable expectation of privacy,"<sup>125</sup> and the answer resides in understanding that "the underlying command of the Fourth Amendment is always that searches and seizures be reasonable."<sup>126</sup> Whether email disclosure analysis within *Warshak* is correct

partially depends on whether the SCA is interpreted according to society's email privacy expectations of today, or those of years past.

Email content classifications that rely on the *age of a message*, or the interpretation of *backup protection*, determine whether the government must compel disclosure using a warrant, a § 2703(d) court order, or a subpoena, which in turn affects whether the government can request a delay of notice to the email subscriber pursuant to § 2705.<sup>127</sup> Reasonable arguments can be made for various interpretations of the SCA,<sup>128</sup> but just as the technology behind email matures, so to must the understanding of society's expectations of email privacy, and the law that enforces those expectations.<sup>129</sup>

Comparing email to a sealed package held by a third party appears to be an appropriate analogy for determining society's privacy expectations.<sup>130</sup> The effect will be that more content will be considered as being in electronic storage, which will trigger the SCA's more restrictive requirements for compelling disclosure.<sup>131</sup>

The theory that disclosure of records to a third party eliminates the reasonable expectation of privacy is valid and applicable in many instances, such as employee email, electronic bulletin boards, and unsecured content,<sup>132</sup> but the burden of proof will be placed on the government to demonstrate that an expectation of privacy has been waived between a subscriber and a provider. The effect will be that the government will be required to provide subscribers with notice more often before using § 2703(d) court orders to compel disclosure, and sections of the SCA deemed to violate the Fourth Amendment will be voided as unconstitutional by the courts, and will need to be revised.<sup>133</sup>

As more electronic communications privacy issues are adjudicated, a greater understanding of society's privacy expectations and exceptions will develop.<sup>134</sup> The effect will be that the particularity requirement of the Fourth Amendment will lead to creation of criteria to identify the purpose and intent of individual messages.<sup>135</sup> Compelled disclosure will move away from providing the government with entire files or databases of content, and towards selection of individual messages that match search criteria provided by the government and processed by a provider.<sup>136</sup> The courts will approve automated searches more readily, applying a threshold of less than probable cause, but the search criteria and procedures will narrowly restricted.<sup>137</sup>

Distinctions related to the age of the message, or whether the message has been accessed by the subscriber, or the type of storage a message is in, will be given less consider-



ation or ignored more often by the courts, leading to calls for legislative revision.<sup>138</sup> The effect will be that more emphasis will be placed on how society uses email, and less emphasis will be placed on artificial classifications that lead to unreasonable decisions.<sup>139</sup>

Clarification of the level of email privacy that society recognizes as reasonable will evolve as electronic communication use becomes more sophisticated, and as technology advances.<sup>140</sup> The effect will be scholarly documents, court opinions, and federal statutes that strive to anticipate technological advances in communications, always seeking to balance “the need to search against the invasion which the search entails.”<sup>141</sup>

In my opinion, email disclosure analysis within *Warshak* was correct, but introduces significant law enforcement concerns that are not easily resolved using existing statutes and case law. The reasoning behind *Warshak* will encourage similar cases in other federal circuits, and Congress will be tasked to respond with updates to ECPA and the SCA that are more consistent with Fourth Amendment protections.

## Conclusion

“E-mail has literally transformed the manner in which American society communicates, and members of society clearly have a vital interest in preserving the privacy of the contents of their e-mails.”<sup>142</sup> The Stored Communication Act creates statutory privacy rights for users of electronic communications, and requirements for disclosure of those same electronic communications to the government. Prosecutors, subscribers, technologists, customers, providers, courts, legislators and commentators struggle to satisfy, interpret, enforce, improve or bypass this set of Fourth Amendment like protections.

18 U.S.C. § 2703 defines requirements for disclosure of customer communications or records to the government. Recent court decisions, including *Warshak v. U.S.*, have surfaced privacy concerns, including whether subsections of the Stored Communications Act violate the Fourth Amendment when ex parte search and seizure orders are authorized on less than a showing of probable cause. Though the government has presented reasonable arguments for maintaining § 2703 procedures, Fourth Amendment protections appear to weigh in favor of voiding offending subsections.

New technologies are developing faster than the applicable legislation, and are presenting new challenges to law enforcement efforts, legislators and judges. In the short term, court decisions may cause prosecutors to lose access to some

of the search and seizure tools the government currently relies upon. Over the long term, “[t]o ensure the continued vitality of the Fourth Amendment . . . the law must advance with technology,”<sup>143</sup> in order to balance the government’s need to search and society’s reasonable expectation of privacy. ■

## About the Author

Michael Gallo is an eighteen year veteran of the information technology industry, employed as a full-time consultant by a Fortune 500 corporation that provides information technology and business process outsourcing services worldwide. Michael holds an M.B.A., an M.S. in Computer and Information Systems, and expects to receive a Juris Doctor in May 2009 from the University of Detroit Mercy School of Law.

## Endnotes

- 1 WILLIAM E. HARTSFIELD, INVESTIGATING EMPLOYEE CONDUCT §6:9 (Nov. 2007).
- 2 Robert S. Steere, *Keeping “Private E-Mail” Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 Val. U.L. Rev. 231, 231 (1998).
- 3 WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, CRIMINAL PROCEDURE, §4.4(c) (3<sup>rd</sup> ed. 2008). “No part of today’s society needs more protection from the exercise of government power than the greatly increasing number of citizens who communicate by sending and receiving electronic mail via the Internet.” Steere, *supra* note 2, at 246.
- 4 Rebecca Porter, *Account Holder Has Right to E-Mail Privacy, Sixth Circuit Rules*, TRIAL, 71, 71 (Oct. 2007).
- 5 U.S. v. Bianco, 998 F.2d 1112, 1124 (2d Cir. 1993).
- 6 Joshua A. Altman, *A Schrödinger’s Onion Approach to the Problem of Secure Internet Communications*, 7 WASH. U. GLOBAL STUDIES L. REV. 103, 107 (2008).
- 7 Steere, *supra* note 2, at 232.
- 8 S. REP. NO. 99-541, at 5 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3559. The Senate Judiciary Committee continued: “Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.” *Id.*
- 9 490 F.3D 455 (6th Cir. 2007) *vacated for rehearing en banc*, 2007 U.S. App. LEXIS 23741 (2007).
- 10 U.S. DEPT. OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, III.A (2002).



- 11 *Id.*
- 12 18 U.S.C.A. § 2701(a) (West 2008).
- 13 18 U.S.C.A. § 2701(b) (West 2008).
- 14 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.D.
- 15 A fourth means to compel providers to disclose information consists of “[o]ne small category of information [that] can be compelled under ECPA without [even] a subpoena. When investigating telemarketing fraud, law enforcement may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing.” U.S. DEPT. OF JUSTICE, *supra* note 10, at III.D. See 18 U.S.C. § 2703(c)(1)(D).
- 16 In two instances, the SCA permits the government to compel information using a mere subpoena: the disclosure of basic subscriber information (as listed in 18 U.S.C. § 2703(c)(2)) and the disclosure of information outside the scope of ECPA. U.S. DEPT. OF JUSTICE, *supra* note 10, at III.D.
- 17 *Id.*
- 18 *Id.*
- 19 18 U.S.C.A. § 2703(d) (West 2008).
- 20 *Id.*
- 21 18 U.S.C.A. § 2510(8) (West 2008) (emphasis added).
- 22 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.C.3. Examples of *non-content* information are listed in 18 U.S.C. § 2703(c)(2), and include the subscriber or customer’s name, address, connection records, session times, telephone number, network address, and means or source of payment for services.
- 23 18 U.S.C.A. § 2510(12) (West 2008) (emphasis added). Electronic communication includes email.
- 24 18 U.S.C.A. § 2510(15) (West 2008). Electronic mail companies and telephone companies are generally considered providers of electronic communication services. See S. REP. NO. 99-541, at 5.
- 25 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.B. Merely forwarding communications being sent by another provider does not qualify as an electronic communication service.
- 26 18 U.S.C.A. § 2711(2) (West 2008). “Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees.” U.S. DEPT. OF JUSTICE, *supra* note 10, at III.B. “In contrast, providers whose services are open only to those with a special relationship with the provider are not available to the public. For example, employers may offer network accounts only to employees.” *Id.*
- 27 18 U.S.C.A. § 2510(14) (West 2008).
- 28 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.B.
- 29 18 U.S.C.A. § 2510(17)(A) (West 2008) (emphasis added).
- 30 18 U.S.C.A. § 2510(17)(B) (West 2008) (emphasis added).
- 31 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.B.
- 32 *Id.*
- 33 *Id.*
- 34 LAFAVE, ET AL., *supra* note 3, §4.8(d).
- 35 *Fraser v. Nationwide Mut. Ins.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001), *aff’d on other grounds*, 352 F.3d 107 (3d. Cir. 2003). See *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y.2001). See also, H.R. REP. NO. 99-647, at 64-65 (1986) (suggesting opened email be covered by RCS provisions).
- 36 LAFAVE, ET AL., *supra* note 3, §4.8(d).
- 37 *Id.*
- 38 *Id.*
- 39 *Theofel v. Farey Jones*, 359 F.3d 1066, 1075 (9th Cir. 2003).
- 40 *Id.*
- 41 LAFAVE, ET AL., *supra* note 3, §4.8(d).
- 42 490 F.3D 455 (6th Cir. 2007) *vacated for rehearing en banc*, 2007 U.S. App. LEXIS 23741 (2007).
- 43 LAFAVE, ET AL., *supra* note 3, §4.8(d). See e.g., *Warshak*, 490 F.3D at 475.
- 44 18 U.S.C.A. § 2703(b)(1) (West 2008).
- 45 18 U.S.C.A. § 2703(b)(1)(A) (West 2008).
- 46 18 U.S.C.A. § 2703(b)(1)(B)(i) (West 2008).
- 47 18 U.S.C.A. § 2703(b)(1)(B)(ii) (West 2008).
- 48 LAFAVE, ET AL., *supra* note 3, §4.8(d), n.28. See *U.S. v. Trimble*, 968 F.2d 394, 399 (10th Cir. 1993).
- 49 LAFAVE, ET AL., *supra* note 3, §4.8(d), n.28.
- 50 Section 2703(d) also applies to non-content records for ECS or RCS.
- 51 Determination of ‘specific and articulable facts’ is interpreted in *Terry v. Ohio*, 392 U.S. 1, 21 (1968).
- 52 18 U.S.C.A. § 2703(d).
- 53 H.R. REP. NO. 102-827, at 31 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3511 (quoted in full in *U.S. v. Kennedy*, 81 F. Supp. 2d 1103, 1109 n.8 (D. Kan. 2000)).
- 54 18 U.S.C.A. § 2703(b)(1)(B)(ii).
- 55 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.D.2.
- 56 The government must determine whether the service provided classifies as electronic communication ser-

- vice, remote computing service, or neither.
- 57 The government must determine whether the information sought is ‘content in electronic storage’, ‘content held by a remote computing service’, ‘non-content subscriber information’, or other ECPA regulated information.
- 58 The government must determine whether the means to compel should be a warrant, a § 2703(d) court order, or an administrative subpoena.
- 59 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.A.
- 60 *Warshak v. U.S.*, Case No. 1:06-CV-357, 2006 U.S. Dist. LEXIS 50076 (S.D. Ohio July 21, 2006).
- 61 *U.S. v. Watson*, 423 U.S. 411, 416 (1996) (quoting *U.S. v. Di Re*, 332 U.S. 581, 585 (1948)).
- 62 *Warshak*, 2006 U.S. Dist. LEXIS 50076 at \*2.
- 63 *Id.* at \*3.
- 64 *Id.* at \*4.
- 65 Non-content information requested included log files, backup tapes, and customer account identifiers, application information, contact information email addresses, billing information to include bank account numbers and any other information related to the accounts, such as setup and synchronization information. *Id.*
- 66 *Id.* at \*3-5.
- 67 *Id.* at \*3-4.
- 68 *Id.* at \*4-5.
- 69 The government conceded that delay of notice for over a year, **without seeking extensions**, violated *Warshak*’s statutory rights. *Warshak*, 490 F.3d at 461 n.1.
- 70 *Id.* at 461.
- 71 *Warshak*, 2006 U.S. Dist. LEXIS 50076 at \*6-7.
- 72 *Id.* at \*2.
- 73 *Id.* at \*31-32. “The general rule is that an unconstitutional statute, whether federal or state, though having the form and name of law, is in reality no law, but is wholly void, and ineffective for any purpose.” DONALD T. KRAMER, 16A AM. JUR. 2D CONSTITUTIONAL LAW § 203 (2d. ed. 2007).
- 74 *Warshak*, 490 F.3d at 460.
- 75 Porter, *supra* note 4, at 71.
- 76 *Warshak v. U.S.*, No. 06-4092, 2007 U.S. App. LEXIS 23741, \*1-2 (6th Cir. Oct. 9, 2007).
- 77 *Warshak v. U.S.*, *Defendants’ Reply to Supplemental Response of the United States to Section II of Defendants’ Omnibus Pretrial Motions*, No. 06-CR-00111-SAS, 2007 WL 4984079 (Nov. 5, 2007).
- 78 *Warshak v. U.S.*, 532 F.3d 521, 523 (6th Cir. 2008).
- 79 *Id.* at 534.
- 80 *Warshak*, 2006 U.S. Dist. LEXIS 50076 at \*8-19.
- 81 *Id.* at \*13.
- 82 *Id.* (quoting *U.S. v. Ross*, 456 U.S. 798, 811-12 and n.16 (1982)).
- 83 Robert M. Goldstein & Martin G. Weinberg, *The Stored Communications Act and Private E-Mail Communications: The Government’s Unconstitutional Policy of Seizing Private E-Mails without a Warrant or Notice*, CHAMPION, 31-AUG CHAMPION 18, 19 (Aug. 2007).
- 84 *Id.*
- 85 *Warshak*, 2006 U.S. Dist. LEXIS 50076 at \*13-14. “The contents of an e-mail are not visible to the naked eye; rather, there are several intrusive searches that axiomatically precede one’s ability to view the contents of an e-mail stored on an ISP’s server.” Goldstein & Weinberg, *supra* note 81, at 19.
- 86 *Id.* at \*14-15.
- 87 *Id.* at \*16.
- 88 *Id.* at \*18-19.
- 89 *Warshak*, 490 F.3d at 461. *See also*, *U.S. v. Long*, 64 M.J. 57 (C.A.A.F. 2006) (finding subjective expectation of privacy in e-mail stored on government server).
- 90 *Warshak*, 532 F.3d at 530.
- 91 *Id.*
- 92 *Warshak*, 490 F.3d at 468.
- 93 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.A, n.14.
- 94 *Warshak*, 490 F.3d at 469. Individuals generally do not enjoy an expectation of privacy in email delivered to a recipient. *See e.g.*, *U.S. v. Lifshitz*, 369 F.3d 173 (2d Cir. 2004).
- 95 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.A, n.14. This theory is based on principles in *U.S. v. Miller*, 425 U.S. 435, 440-43 (1976) (holding that bank records were disclosed information and thus not subject to Fourth Amendment protection), and *Smith v. Maryland*, 442 U.S. 735, 741-46 (1979) (finding no reasonable expectation of privacy in dialed telephone numbers). *Id.*
- 96 *Warshak*, 490 F.3d at 469.
- 97 Porter, *supra* note 4, at 71.
- 98 *Warshak*, 490 F.3d at 469.
- 99 LAFAYETTE, ET AL., *supra* note 3, §4.4(c).
- 100 *Warshak*, 490 F.3d at 470.
- 101 *Id.* at 471. In *U.S. v. Maxwell*, the ISP’s “policy was not to read or disclose subscribers’ e-mail to anyone except authorized users, thus offering its own contractual privacy protection in addition to any federal statutory protections.” *U.S. v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996).

- 102 LAFAVE, ET AL., *supra* note 3, §4.4(c).
- 103 *Id.*
- 104 *Warshak*, 490 F.3d at 473.
- 105 *Warshak*, 532 F.3d at 526.
- 106 *Id.* at 527.
- 107 LAFAVE, ET AL., *supra* note 3, §4.4(e).
- 108 *Id.*
- 109 *Id.*
- 110 Peter S. Kozinets, *Access to the E-Mail Records of Public Officials: Safeguarding the Public's Right to Know*, COMMUNICATIONS LAWYER, Summer 2007 at 22. See Jennifer LaFleur, *Ruling: Dallas officials' e-mails must be turned over*, THE DALLAS MORNING NEWS (Oct. 30, 2007), <http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/102907dnmetemails.317323a.html> (last visited Apr. 13, 2008).
- 111 *Warshak*, 490 F.3d at 476, n.8.
- 112 *Id.*
- 113 *Id.* See generally, *U.S. v. Maxwell*, 45 M.J. at 417 (tenor and content of email revealed reasonable expectation that conversations were private).
- 114 *Warshak*, 490 F.3d at 476, n.8.
- 115 LAFAVE, ET AL., *supra* note 3, §4.4(c).
- 116 *Id.*
- 117 *Id.* The government typically obtains a warrant before opening unopened mail. *Id.* at n.13. See, e.g., *U.S. v. Barr*, 605 F. Supp. 114 (S.D.N.Y. 1985) (permitting a subpoena to obtain postal mail, although not reaching the process required to open postal mail, because a warrant was obtained).
- 118 See, e.g., *U.S. v. Lamb*, 945 F. Supp. 441, 458-59 (N.D.N.Y. 1996) (applying the particularity requirement), *U.S. v. Maxwell*, 45 M.J. at 422 (applying the plain view doctrine). See generally, *U.S. v. Bach*, 310 F.3d 1063 (8th Cir. 2002) (applying the Fourth Amendment to the process of obtaining customer e-mail from an ISP).
- 119 LAFAVE, ET AL., *supra* note 3, §4.4(c).
- 120 *Warshak*, 2006 U.S. Dist. LEXIS 50076 at \*19, n.11.
- 121 LAFAVE, ET AL., *supra* note 3, §4.8(d).
- 122 *Id.* A challenging question is whether a message accessed by a subscriber and kept on a provider's server is protected under § 2703(a) as electronic storage, or should be protected by § 2703(b) as a file held by a remote computing service. *Id.*
- 123 *Katz v. U.S.*, 389 U.S. 347, 360 (1967). "[W]hether a defendant's expectation of privacy is one that society is prepared to recognize as reasonable is a question of law subject to de novo review." *U.S. v. Clark*, 22 F.3d 799, 801 (8th Cir. 1994).
- 124 U.S. DEPT. OF JUSTICE, *supra* note 10, at III.A.
- 125 *Porter*, *supra* note 4, at 71.
- 126 *Bianco*, 998 F.2d at 1124.
- 127 See *supra* Section I.C.
- 128 See *supra* Section II.B.1-2.
- 129 See *supra* Introduction.
- 130 See *supra* Section II.B.1.
- 131 See *supra* Section I.C.
- 132 See *supra* Section II.B.2.
- 133 See *supra* Section II.A, n.73.
- 134 See *supra* Introduction, n.3, n.8.
- 135 See *supra* Section II.C, n.107.
- 136 See *supra* Section II.C.
- 137 *Id.*
- 138 See *supra* Section II.C, n.8.
- 139 See *supra* Introduction, Section II.C, n.3, n.89, n.94, n.101, n.113.
- 140 See *supra* Introduction, Section II.C, n.123. The convergence of email, text messaging, voice mail, instant messaging, faxing, voice and video streaming, teleconferencing, videoconferencing, and blogging will enable electronic communications to be available through an endless variation of devices, using ever improving security systems, and processed by an overlapping network of providers and architecture. Instead of sending entire messages through providers, notifications will be sent, and secure, on-demand retrieval through peer-to-peer devices will provide individuals absolute control over communication exchange and storage. *Author's opinion.*
- 141 *Bianco*, 998 F.2d at 1124.
- 142 *Goldstein & Weinberg*, *supra* note 81, at 18.
- 143 *Steere*, *supra* note 2, at 265.

## Meet a Section Member: **Jeremy D. Bisdorf**

- **What is the name of your firm/corporation/employer**  
Jaffe, Raitt, Heuer & Weiss, Professional Corporation
- **What is your area of practice?**  
Intellectual property, Business and Information technology
- **When did you first become involved with the Section?**  
Joined in 2000. Elected to Council in 2005. Entered officer track in 2006 as Treasurer. Currently serving as Chair-Elect.
- **Where did you grow up?**  
Sterling Heights, Michigan
- **Where else have you lived?**  
Detroit, Ann Arbor and now, Northville.
- **Where did you attend undergraduate and law school?**  
Wayne State University - Undergraduate and Master of Laws in Taxation  
The University of Michigan Law School - Juris Doctor
- **What was your undergraduate major?**  
Finance and Business Economics
- **What are your hobbies, other interests?**  
Studying my faith, spending time with my family doing whatever, coaching little league baseball, Wii, golf
- **Favorite restaurant?**  
Don Shula's Steakhouse
- **A recent book you read?**  
*On the Way to Jesus Christ* by Pope Benedict XVI
- **Last vacation?**  
Walt Disney World, last February
- **Favorite legal case (with a tie to Michigan) that can be found in Westlaw or Lexis?**  
LUCAS NURSERY AND LANDSCAPING, INC. v. GROSSE, 359 F.3d 806 (6th Cir., 2004).  
  
While I am not a litigator, I assisted on this case with a couple of lawyers who remain good friends and we won one for the little guy.
- **Who is your hero? (a parent, a celebrity, an influential person in one's life)**  
Father John Riccardo, the pastor of Our Lady of Good Counsel Church in Plymouth, Michigan.
- **If you had to describe yourself using three words, they would be...**  
Husband, Father, Lawyer
- **What is your favorite movie of the past ten years?**  
The Passion of the Christ.
- **What do you like to do most with a free hour?**  
Read
- **What is the most significant event of your life in the last three months?**  
The birth of my son, Jonathan, and his subsequent medical care provided through Mott's Children's Hospital at the University of Michigan in Ann Arbor.
- **What one word would you put on your gravestone?**  
Redeemed
- **What email can Section members use to contact you?**  
[jbisdorf@jaffelaw.com](mailto:jbisdorf@jaffelaw.com)
- **A short comment on why you became involved with the Information Law Technology Section:**  
To network with professionals engaged in similar areas of the law and establish relationships and learn from them ■

---

## Publicly Available Websites for IT Lawyers

The Proprietary Rights Committee of the Information Technology Law Section has assembled a list of over 50 publicly available websites with up-to-date, reliable and comprehensive information that is useful to lawyers who practice in the IT law area. The websites are easy to search or navigate to obtain the desired information, and although raw data and information are important, often the websites contain summaries and discussions, as well as links to other useful websites.

The Michigan IT Lawyer will publish a selection of these websites in each issue, and feedback or recommendations for additional websites can be forwarded to David Syrowik, [DSyrowik@brookskushman.com](mailto:DSyrowik@brookskushman.com). Enjoy!

### Statutes

- <http://thomas.loc.gov> - federal legislative information
- <http://www.ucitaonline.com> or <http://www.nccusl.org> - software licenses, UCITA and its provisions
- <http://www.ucita.com> - opposition to UCITA.

### Case Law

- <http://www.altlaw.org> - free searchable database of Supreme Court and Federal Appellate case reports. Among the searchable are appellate and Supreme Court opinions for the last 40 to 50 years. AltLaw is claimed to be updated daily.
- <http://lp.findlaw.com> - this is 'FindLaw for Legal Professionals,' rather than FindLaw's non-legal web site designed for consumers

### Domain Name Registration

- <http://www.iana.org/root-whois/index.html> - list of the current country code domains and links to their registries and registry contacts
- <http://www.icann.org/registrars/accredited-list.html> - a list of all registrars accredited to register universally recognized domain names
- <http://www.icann.org/en/dndr/udrp/policy.htm> - ICANN dispute resolution policy that applies to all domain names
- <http://www.icann.org/en/dndr/udrp/approved-providers.htm> - links to approved dispute resolution providers
- <http://www.networksolutions.com/whois> - NSI's database to determine if a domain name is available
- <http://www.uspto.gov/web/offices/tac/domain> - a position paper on registering domain names. ■



## 2009 Edward F. Langs Writing Award

### Essay Competition Rules

1. Awards will be given to up to three student essays, which in the opinion of the judges make the most significant contribution to the knowledge and understanding of information technology law. Factors to be taken into consideration include: originality; timeliness of the subject; depth of research; accuracy; readability; and the potential for impact on the law
2. Essay must be original, deemed to be of publishing quality, and must not have been submitted to any other contest within the previous 12 months.
3. Essay must be typed, double spaced, at least ten pages in length, must contain proper citations listed as either endnotes or footnotes, and must have left, right, top and bottom margins of one inch.
4. Essay must include the submitter's name, email address, mailing address, telephone number, and school attended.
5. A total of \$1,500 in US dollars shall be divided between the award winning essays, and all rights to award winning essays shall become the property of the State Bar of Michigan.
6. The Information Technology Section of the State Bar of Michigan reserves the right to make editorial changes, and to publish award winning essays in the Section's newsletter, the *Michigan IT Lawyer*.
7. Essay must be submitted as a Microsoft Word document, postmarked by June 30, 2009, and emailed to **DSYROWIK@brookskushman.com**