

## Overseas Court Decisions Limit U.S. Internet Speech

*Foreign Courts' Decisions to Exercise Jurisdiction over Internet Libel Claims Presents a Free Expression, and e-Commerce, Challenge*

By Jonathan Bick

Australian, English and Canadian court rulings associated with defamatory Internet communications emanating from the United States may limit American speech, a specter that stands to cast a long, haunting shadow over a range of U.S.-based activities, from publishing to online auctions to discussion and criticism.

For jurisdictional purposes, Internet publications may be subject to worldwide legal difficulties. Using common law theory, foreign courts have found American Internet publishers liable for harm to readers located in foreign jurisdictions, and have subjected those publishers to foreign-liability law, even though American law holds the sender immune from liability.

### TWO-PRONGED CHALLENGE

Foreign jurisdiction over controversies associated with American Internet publications presents two distinct legal difficulties.

First, foreign jurisdiction requires Americans to travel outside the United States to participate in a process to resolve a controversy or face default.

*continued on page 5*

## Tools to Save Time That You Do Not Have

*You Won't Make Time if You Don't Save Time*

By Stanley P. Jaskiewicz

Today, it seems that anyone involved in e-commerce must be online and available, all the time. You know how it is because you live it: Blackberries and Internet-enabled cell phones provide instant delivery of e-mail, wherever you may be — whether working, or spending time with family and friends. Online etiquette seems to require that you reply instantly, regardless of your other responsibilities or non-work-related activity in which you may be engaged.

Clients demand instantaneous response and around-the-clock availability. With online access, a cell phone call that may not get through or be answered just isn't fast enough.

In one extreme case in my own experience, an attorney replied that he would be unable to discuss a pending deal within seconds after my message, explaining that he was in the delivery room with his wife, who was in labor. Fortunately for him (and his marriage), he quickly broadcast a message that he would be unavailable for several days, after I pointed out that the birth of his child might be more worthy of his attention than his BlackBerry.

But the fact that he was even checking e-mail at a time when most of us would prefer to experience and remember that special moment shows how intense the pressure for around-the-clock availability can be for those in the e-commerce economy. Perhaps there's no place in e-commerce for "living in the moment."

### DON'T GET STRANDED, PLOT A COURSE

Instead, those keyboarding on this e-commerce treadmill have time to think only about the e-mail that may arrive — and dream of relocating to a modern-day equivalent of Gilligan's Island: "No phone, no lights, no motor cars, not a single luxury" (for a blast from the past, see, [http://en.wikipedia.org/wiki/Gilligan's\\_Island](http://en.wikipedia.org/wiki/Gilligan's_Island)) — and no e-mail, a modern "convenience" that Gilligan and his companions stranded after that 3-hour tour in the mid-1960s couldn't have dreamed of. Indeed, we lose the joy of focusing on our immediate experience, like the birth of a child, rather than on

*continued on page 2*

### In This Issue

Tools to Save Time That You Do Not Have . . . 1

Overseas Court Decisions Limit U.S. Internet Speech . . . 1

Europe's Reaction Against the SOX Anonymous Whistleblowing Rule . . . 3

New Kinds of e-Commerce . . . 7

e-Commerce Docket Sheet . . . 11

## Save Time

continued from page 1

what has happened, or what might happen. We never experience “mindfulness” — “not judging, reflecting or thinking (but) simply observing the moment in which you find yourself” (see, [www.mindfulness.com](http://www.mindfulness.com)).

For most of us, constant connectiveness is no longer just a way of life — it’s a job requirement, and the only way to survive. The quick e-mail reply can become the difference between keeping and losing a client and, ultimately, between sanity and burnout. Everyone in our world scrambles to save time — even a few minutes here and there — to satisfy client expectations. Only after those obligations are met, if ever, can we perhaps hoard a few minutes for ourselves.

### MAKING THE MOST OF WHAT YOU HAVE

In the face of these time pressures, however, it’s surprising how many e-commerce practitioners, or their counsel, don’t use the many time-saving efficiencies that are readily available. Even though many are free or built into the applications we use every day, I don’t see them active on the computers of colleagues or clients.

For this article, I’ve assumed a Windows operating system with an always-on, high-speed Internet connection and an Internet Explorer browser, with a true e-mail program such as Outlook — rather than Web-based mail such as Hotmail or G-mail, or mail retrieved through a PDA.

And it’s not simply a mind frame that practitioners of e-commerce, or those who provide them with legal and business counsel, must foster or even adopt unknowingly — the use of e-

**Stanley P. Jaskiewicz**, a business lawyer, helps clients solve e-commerce, corporate, contract and technology-law problems, and is a member of *e-Commerce Law & Strategy*’s Board of Editors. He can be reached at the Philadelphia law firm of Spector Gadon & Rosen P.C., at [sjaskiewicz@lawsgr.com](mailto:sjaskiewicz@lawsgr.com), or at 215-241-8866.

commerce tools has become pretty much ubiquitous. For example, many people never change the “out-of-the-box” configuration of Outlook or Internet Explorer — that is, the way the program appears on their screen. Certainly, the browser buttons and other aspects of their browsers’ appearance are valuable electronic real estate. The maxim “location, location, location” applies to the cyber world even more so than to the realm of real estate — and advertisers pay dearly to be included in the pre-configured versions of software that appear on installation. What could be more valuable to e-commerce advertisers than the space on the screen that potential customers view all day, every day?

Yet, many don’t know how easy it is to delete pre-selected buttons that you don’t need or want, despite the cost to the sponsors for placement. You can remove them, and add your own preferences, by right-clicking on each link button, and selecting “delete.” You can also provide yourself quick access to programs you use every day by enabling the “quick launch” or “desktop” options in the taskbar at the bottom of the screen, so that you can launch programs without leaving a Web page or e-mail program.

Most applications permit easy customization to introduce features that, over the course of a day, will save time that accumulates. Clients are also impressed when, during the course of a phone call, you can quickly locate the news article they’re asking about or run an informal search at a public-records site to provide more information about their question, without wasting time to manually search Web sites — once you find the sites. An e-commerce lawyer often must be as much of a librarian and researcher as an advocate and fighter.

### BUILDING YOUR OWN E-TOOLBOX

Consider: In Internet Explorer, the “Links” toolbar, from the drop-down “View” menu, provides one-click access to one’s favorite sites. (The button, or “Links” bars, appears under the “View” drop-down menu, under “Toolbars” and “Links.”) These are

continued on page 6

## e-commerce LAW & STRATEGY®

EDITOR-IN-CHIEF	.....Michael Lear-Olimpi
EDITORIAL DIRECTOR	.....Wendy Kaplan Ampolsk
MANAGING EDITOR	.....Steven Salkin, Esq.
MARKETING DIRECTOR	.....Colin Graf
MARKETING PROMOTIONS	
COORDINATOR	.....Rob Formica
MARKETING ANALYSIS	
COORDINATOR	.....Traci Footes
GRAPHIC DESIGNER	.....Crystal Hanna
BOARD OF EDITORS	
RICHARD BUCHBAND	.....Juno Online Services Inc. New York
JEFFREY P. CUNARD	.....Debevoise & Plimpton Washington, DC
WALTER A. EFFROSS	.....American University Washington, DC
MARIE FLORES, J.D.	.....Southwest Bank of Texas Houston
D. REED FREEMAN JR.	.....Claria Corp. Washington, DC
ELIZABETH A. GAUDIO	.....Nat’l Federation of Ind. Bus. Legal Foundation Washington, DC
BRUCE GAYLORD	.....JPMorgan Chase Bank New York
PAUL R. GUPTA	.....Mayer, Brown, Rowe & Maw New York
THOMAS HEYMANN	.....Willke, Farr & Gallagher Frankfurt, Germany
STANLEY P. JASKIEWICZ	.....Spector Gadon & Rosen, P.C. Philadelphia
PHILIPPA LAWSON	.....Canadian Internet Policy and Public Interest Clinic Ottawa
EMILE LAZO	.....Technology Law Group Boise, ID
JULIAN S. MILLSTEIN	.....Brown Raysman Millstein Felder & Steiner New York
JEFFREY D. NEUBURGER	.....Brown Raysman Millstein Felder & Steiner New York
EDWARD A. PISACRETA	.....Brown Raysman Millstein Felder & Steiner New York
LUIS SALAZAR	.....Greenberg Traurig LLP Miami
HOWARD SIEGEL	.....Pryor Cashman Sherman & Flynn LLC New York
J.T. WESTERMEIER, JR.	.....DLA Piper Rudnick Gray Cary Northern Virginia
JOSEPH P. ZAMMIT	.....Fulbright & Jaworski New York

e-Commerce Law & Strategy® (ISSN 0747-8933) is published by Law Journal Newsletters, a division of ALM. © 2006 ALM Properties, Inc. All rights reserved. No reproduction of any portion of this issue is allowed without written permission from the publisher. Telephone: (800) 999-1916  
Editorial e-mail: [ssalkin@alm.com](mailto:ssalkin@alm.com)  
Circulation e-mail: [subspa@alm.com](mailto:subspa@alm.com)

The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.

e-Commerce Law & Strategy P0000-236  
Periodicals Postage Pending at Philadelphia, PA  
POSTMASTER: Send address changes to:  
ALM  
1617 JFK Blvd., Suite 1750, Philadelphia, PA 19103  
Annual Subscription: \$395

Published Monthly by:  
Law Journal Newsletters  
1617 JFK Boulevard, Suite 1750, Philadelphia, PA 19103  
[www.ljonline.com](http://www.ljonline.com)

# Europe's Reaction Against the SOX Anonymous Whistleblowing Rule

## *The Act and EU Regulations Conflict in Some Ways, Pending a Resolution*

By Daniel P. Westman

Watching the reaction of European data-protection authorities to the anonymous whistleblower requirement set forth in §304 of the Sarbanes-Oxley Act of 2002 (SOX) has been like watching an ongoing heavy-weight prize fight.

In one corner, representing the United States and its recent history of corporate frauds, stands the SOX champion determined to use all means to prevent future frauds.

In the other corner, representing Europe's 20<sup>th</sup>-century history, which, unfortunately, includes use of anonymous "informants" to "denounce" and silence or kill opponents of repressive regimes in Germany, France and elsewhere, stands the European Union (EU) data-protection champion resolved to protect what Europeans view as the fundamental human right of privacy.

The SOX and EU champions have exchanged blows, neither has given up much ground, and the match appears to be headed into the late rounds.

The audience of multinational corporations required to comply with SOX and EU data-protection laws — whether in e-commerce or bricks-and-mortar operations — can only

---

**Daniel P. Westman** is a partner in the McLean, VA, office of Morrison & Foerster LLP. He is the principal author of *Whistleblowing: The Law of Retaliatory Discharge, Second Edition* (BNA Books, 2004 & 2005 Supp.). The author gratefully acknowledges the contributions of **Miriam Hauser Wugmeister**, **Karin Retzer** and **La Tanya N. James** to this article. Westman can be reached at [dwestman@mofo.com](mailto:dwestman@mofo.com).

watch, do their best to implement anonymous whistleblower mechanisms in compliance with both SOX and EU privacy law, and wait until the contest is decided.

### SOX'S OPENING SALVO

Section 304 requires the audit committees of boards of directors of publicly traded companies to establish mechanisms for "receipt, retention and treatment" of anonymous employee concerns about potential accounting improprieties or fraud against shareholders. Section 304 is one of the rare instances in U.S. law in which anonymous whistleblowing is specifically protected by law. Congress determined that encouragement of anonymous whistleblowing was a necessary element of SOX's overall framework aimed at deterring fraud against shareholders. The full scope of SOX's scheme of "undersight," which is shorthand for protection for corporate insiders who raise concerns about shareholder fraud, is discussed in this author's article, "Compliance in the Era of 'Undersight'" in the July 2005 edition of our sibling publication, *The Corporate Compliance & Regulatory Newsletter*. (See also, "Is Your Hotline AAA-Rated?", in the April edition of *e-Commerce Law & Strategy*.)

The theory behind creating legal protection for anonymous whistleblowing is to provide employees with a means of raising concerns about fraud without fear of having their employment terminated in retaliation. In the United States, with its flexible labor market premised on employment "at will," under which either the employer or employee may terminate the relationship at any time for any reason, whistleblowing employees might well fear being fired if their identities were known — and might desire the protection of anonymity. Fired whistleblowers are not automatically entitled to severance payments under U.S. law, and must seek remedies in the courts, and risk the uncertainties surrounding litigation.

### THE EU'S COUNTERPUNCH

Many U.S.-based companies subject to SOX have taken anonymous whistleblower mechanisms designed for America and have implemented them in their EU operations, without

any revision to take into account EU data-protection laws. Section 304 has collided with EU data-protection law in several respects. In 2005, courts in France and Germany ruled against U.S. companies that implemented anonymous whistleblowing mechanisms in those countries. Also, in late 2005 the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, or CNIL) issued guidelines allowing anonymous-whistleblowing mechanisms limited to accounting and fraud issues, but only subject to numerous restrictions.

On Feb. 1, the EU data-protection authority (the Article 29 Working Party, or WP29) issued an opinion allowing use of anonymous whistleblowing mechanisms, subject to restrictions similar to those required by the French CNIL. The WP29 opinion provides guidance to the EU's 25 member states (at present, Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and the United Kingdom).

While the WP29 opinion allows use of anonymous whistleblower mechanisms limited to SOX concerns such as accounting, auditing, banking and financial corruption, the opinion also is apparently inconsistent with §304 in the following respects:

- It recommends that companies encourage employees to identify themselves when making complaints, discourages anonymous employee complaints, not to advertise the existence of anonymous channels, and to clearly inform employees that whistleblowing is voluntary;
- It recommends that use of anonymous channels be limited to employees who have access to accounting, auditing and financial information;
- It recommends that limits be placed on the number of persons against whom anonymous complaints may be filed;
- It requires that certain rights of defense be provided to persons accused of wrongdoing;

*continued on page 4*

*continued from page 3*

- It recommends erasure of inaccurate data, and destruction of all data after 2 months, which appears inconsistent with §304's requirement that audit committees establish procedures for "receipt, retention and treatment" of anonymous complaints;
- It advises that employees should be notified that allegations made in bad faith may result in disciplinary action or legal proceedings by persons falsely accused;
- It recommends the creation of a separate organization, apart from the human resources department, consisting of specifically trained personnel to investigate employee complaints;
- It recommends that companies should "deal with reports locally, *ie*, within one EU country, rather than automatically share all the information with other companies in the group"; and
- It recommends that personal data not be transferred to countries outside the EU that do not have privacy laws equivalent to EU privacy laws, unless companies in such other countries agree to certain privacy requirements.

On Feb. 16, the chairman of WP29 wrote a letter to the chairman of the U.S. Securities and Exchange Commission (SEC) requesting that the SEC provide assurances that companies located in the EU that comply with the opinion will be viewed as having complied with their obligations under SOX. Given the number and importance of the inconsistencies between the opinion and SOX, it's difficult to see how the SEC will be able to provide the requested assurances. As of late July, the SEC and WP29 had been trading letters. The SEC hadn't made its letter public, and it was hard to predict at press time when — if ever — a resolution might be reached. Until then, U.S. and EU companies with EU nation operations must comply with both regulations. Some of the spirit of the SOX anonymous whistleblowing must be compromised, but the letter of SOX may not necessarily be violated in those instances.

## COMPLIANCE STRATEGIES

As this heavyweight match continues, companies with e-commerce and "old-fashioned" operations that seek to comply with EU data-protection laws should consider the following when setting up whistleblowing schemes in the EU:

- Limit the scope of whistleblowing schemes to complaints relating to SOX matters (*ie*, accounting, auditing, banking, and financial corruption);
- Consider disassociating the general ethics code from the reporting scheme;
- Notify employees about the details of the whistleblowing scheme, including the entity responsible for the scheme, the personnel receiving the reports, third-party service providers, the purpose of the scheme, the right to access and modify information reported under the scheme, and the voluntary nature of the scheme;
- Encourage employees to identify themselves while protecting the confidentiality of their identities;
- Ensure that all persons identified in reports are provided with complete information; including a description of the incident and possible recipients, as soon as the evidence is secured;
- Collect reports through a dedicated channel;
- Ensure that reports are either deleted or securely archived if no proceedings of legal action or disciplinary sanctions were initiated within 2 months after making the report;
- Enter into appropriate contracts with providers of reporting services, particularly as regards the confidentiality of information collected, security measures in place, cooperation with requests for access, and rectification and retention policy;
- Provide whistleblowers and implicated employees with the opportunity to access information, and to modify or delete any inaccurate or incomplete information when appropriate; and
- State that misuse of the scheme, *ie*, such as bad-faith allegations, may result in disciplinary actions and legal proceedings.

## HOW MIGHT THE WP29 OPINION AFFECT FRAUD PREVENTION?

One cannot avoid the observation that the many restrictions placed by the WP29 opinion on anonymous-whistleblowing mechanisms reflect a deep European hostility toward "denunciations" by "informants." Compliance professionals might be concerned that the WP29 opinion could have the effect of reducing the flow of information from EU-based employees about potential fraud. It remains to be seen, however, whether this hostility will have much effect on efforts of compliance professionals to prevent fraud in the EU. Unlike the United States, with its flexible labor markets premised on employment at will, many EU member states have relatively inflexible labor markets premised on elaborate job-protection schemes that require payments of certain amounts of severance. The EU data-protection laws require EU employers to provide much higher levels of confidentiality to employees than do U.S. laws. It may be that the EU system — in which the costs of firing employees are higher compared to the at-will regimen of the United States, and in which personal data is given a high level of protection — creates a climate in which EU employees do not feel the need for the protection of anonymity to raise their concerns about financial fraud.

There are other reasons why the WP29 opinion may not reduce the flow of information arising from anonymous complaints about potential fraud in the EU. Although WP29 has not yet opined on this issue, it is possible that anonymous reports made by employees located in the EU, but which are received in the United States, may not be deemed subject to EU data-protection laws. Many U.S.-based companies maintain anonymous telephone hotlines or Web-based mechanisms that can receive reports from anywhere in the world. Indeed, it may not be possible for U.S.-based companies to determine from which country an anonymous telephone call or e-mail originated, particularly if a U.S. company uses a third-party hotline or Web-based

*continued on page 9*

## Internet Speech

continued from page 1

Second, foreign jurisdiction normally results in the use of the law of that foreign jurisdiction.

The downside, as most publishers would see it, is that other than having an Internet publication reviewed by attorneys from every jurisdiction on earth, self-censorship is among the few alternatives available to American Internet publishers seeking to avoid foreign legal difficulties.

### FOREIGN COURT DECISIONS

#### Australia

The High Court of Australia, in *Dow Jones & Co. v. Gutnick*, (2002) 210 C.L.R. 575, for instance, found that Australian jurisdiction applied to a libel action brought by an Australian citizen over assertions of money-laundering published on a New Jersey Web site.

The Australian court rejected defendant Dow Jones' argument that New Jersey's law should be applied simply because New Jersey was the place where the publisher maintained its Web servers. Instead, the High Court of Australia applied traditional common-law principles for determining jurisdiction in libel actions to accommodate the Internet. The court said that those who provide information via the Internet know of the possible far-reaching effects their information may have and, by implication, take the legal risks associated with the dissemination of that information.

Other foreign plaintiffs have successfully applied principles developed for newspapers to Internet publications. In the case of *Berezovsky v. Forbes, Inc.*, (2000) 1 W.L.R. 1004, a person residing in England was permitted to bring libel proceedings in the forum in response to statements in *Forbes* magazine, which had a small circulation in the United Kingdom.

**Jonathan Bick** is of counsel to WolfBlock Brach Eichler of Roseland, NJ, and is an adjunct professor of Internet law at Pace Law School and Rutgers Law School. He is also the author of *101 Things You Need To Know About Internet Law* (Random House 2000).

As a result of the successful application of foreign common law to American Internet publishers, online publishers must consider the libel laws of every country in which their messages could be downloaded. Such widespread threat of suit is likely to interfere with Internet speech.

#### England and Canada

The approach of the English courts in libel cases is similar to that taken by the Australian courts. An English court, in *King v. Lewis*, (2005) E.M.L.R. 4, found that a Florida resident could bring a libel action in England in response to allegations made by the defendants posted on a California Web site. The English court reasoned that the appropriate jurisdiction for a trial was the place where the defamation was committed. As such, the defamatory statements were downloaded in England; however, in a more recent case, *Dow Jones & Co. v. Jameel*, (2005) E.M.L.R. 16, 374-75, an English court dismissed a claim brought in response to libel allegations accessible by hyperlink from *The Wall Street Journal* online. The court said that only two parties not associated with the case had accessed it.

A Canadian court, in *Bangoura v. The Washington Post*, (2004) 235 D.L.R. (4th) 564, applied jurisdictional principles similar to those used by the English and Australian courts. That court reiterated that those who put information on the Internet do so knowing the possible reach of the information.

#### COMMON-LAW CONSIDERATIONS, AND NOT

While the courts in Australia, England and Canada each used common law as a basis for finding jurisdiction, alternative outcomes under common law are possible. Under common law, for example, the place of the tort is often the most appropriate place to hear the case.

Traditionally, the place of "publication" is the place where the statement is read. The courts in Australia, England and Canada each mechanically found that the statement was read in their own countries. Each court failed to find that the publication was, in fact, located outside its country, and that it was necessary for

the reader to electronically "travel" outside his or her country and take action to bring the publication in question back to read it. According to Internet protocol, the transaction is more accurately described as material downloaded from servers on the other side of the world rather than of reading material from afar.

Consequently, the courts in Australia, England and Canada each erroneously applied the precedents relating to print and broadcast publishing, and failed to examine the inherent differences between these traditional methods of publication and the Internet. Had they applied the common-law rule accurately, they would have concluded that jurisdiction was properly in the United States.

#### PARSING DIFFERENCES IN LAW AND APPLICATION

The Australian court questioned whether the Internet was really different from television services, such as satellite broadcasting. The court found that the Internet operates as a broadcasting service, such as CNN or BBC Worldwide, which sends content to recipients. The court did not consider that Internet recipients must locate, visit and send content to themselves (*ie*, download).

Under common law, if a person travels to a foreign jurisdiction and secures a libelous publication, the foreign court has jurisdiction. The fact that such a person subsequently travels to his or her home jurisdiction does not alter the fact that under common law, he or she must take action in the foreign jurisdiction. In short, the Internet is different from traditional forms of publication and broadcasting, and the differences can be used to argue either for or against the application of traditional jurisdiction under common law, which may lead to liability for libel.

Unless courts recognize the novel characteristics of the Internet, *Gutnick*, and other English-court decisions adopting libel jurisdiction and choice of law in Internet cases will allow jurisdiction shopping. In particular, parties will seek the claimant-friendly defamation laws of Australia or England.

continued on page 10

## Save Time

*continued from page 2*

similar to the familiar “Favorites,” but (in my opinion) provide more convenient access. Simply open the desired site in a browser window, and drag the address-bar icon to the links bar. Renaming the links for the sites one uses daily to one- or two-letter abbreviations allows almost 20 short-cuts to appear on a screen at all times.

For my practice, for example, my browser has links to various public-records sites and research services that I find invaluable in due-diligence investigations. S1 and S2 are link farms to the Web site for the National Association of Secretaries of State, where one can link to the Web site of each U.S. state’s Secretary of State ([www.nass.org/sos/sosflags.html](http://www.nass.org/sos/sosflags.html)) and a page at the Law Library Resource Xchange that lists links to state business-filing databases ([www.llrx.com/columns/roundup29.htm](http://www.llrx.com/columns/roundup29.htm)). P1 links to my own state’s public-records filings (<https://www.dos.beta.state.pa.us/CorpsApp/CorpsWeb/wfDefault.asp>), while DE does the same for Delaware (<https://sos-res.state.de.us/tin/GINameSearch.jsp>). Most e-commerce practitioners couldn’t do without buttons to a Whois site, such as <http://whois.domaintools.com> or [www.register.com](http://www.register.com), or even one of the “reverse look-up” sites that allows searching by IP address to get Whois registration information, such as [www.dnsstuff.com](http://www.dnsstuff.com) or [www.domaintools.com/reverse-ip](http://www.domaintools.com/reverse-ip) (requires registration).

I also have specialized research links, in addition to L (for Lexis/Nexis) and W (for Westlaw). P takes me to the U.S. Patent and Trademark Office’s search site, [www.uspto.gov/main/search.html](http://www.uspto.gov/main/search.html), while K leads to a database of contracts disclosed in public-company filings at FindLaw for Small Business, <http://smallbusiness.findlaw.com/business-forms/contracts/contracts/index.html>. Links to many public-records Web sites across the nation are at PR1, for BRB Publications Inc.’s Facts on Demand Press Free Resource Center, and PR2, at [www.brbpub.com/pubrecsites.asp](http://www.brbpub.com/pubrecsites.asp) and [www.searchsystems.net](http://www.searchsystems.net). Other

sites rotate in and out as I need them, such as a client site during a deal, or a child’s sports-team site. Finally, I include frequently used general-reference sites, such as a phone directory, sites for Web-based e-mail, or *The New York Times* reference library ([www.nytimes.com/learning/general/navigator/index.html](http://www.nytimes.com/learning/general/navigator/index.html)). And who can do without this publication’s home site — [www.ljnonline.com/alm?ecomm](http://www.ljnonline.com/alm?ecomm), and the general site for its sibling newsletters, [www.ljnonline.com](http://www.ljnonline.com)? I keep additional Internet resources handy at [www.virtualchase.com/articles.shtml](http://www.virtualchase.com/articles.shtml), as well as general due-diligence sites, such as [www.llrx.com/features/ciguide.htm](http://www.llrx.com/features/ciguide.htm). Links to newspaper Web sites nationally ([www.newspaperlinks.com/home.cfm](http://www.newspaperlinks.com/home.cfm)) help me track down a story a client may have heard about.

### INDIVIDUAL POWER CUSTOMIZATION

Of course, these are the sites that I use frequently. Each person can easily drag and drop the Web sites he or she chooses that are most relevant to his or her own life and practice.

Once your preferred toolbars are set, don’t forget to “lock the toolbars,” another option under the “View” and “Toolbars” drop-down menus. If you want to cram more onto your screen, you can easily change icon and font sizes from the default views under the “View” and “Text Size” or “Toolbars”/“Customize” drop-down menus.

Many toolbars available online (such as the Google and Comcast toolbars) offer another incredibly useful browser time-saver: the “search within a site” button. Frequently, a link from a Web site leads to a home page rather than to the specific page mentioned at the referring site. The ability to search within a site lets you quickly drill down to the appropriate page. While this feature has long been available at the leading search engines, the ability to use it, with one click, right at the moment when you reach the page, may not have been well known, but it saves several steps, and prevents giving up on the search.

Many sites have also recently begun resurrecting the failed “portal”

model from the dot-com era, allowing users to customize a home page with specific content that the user chooses. Presumably, this will preserve loyalty to the site (and generate higher advertising rates and revenue).

But while one can choose such diversions as celebrity magazines and the like, useful information and tools such as a calculator, news feeds or other streaming data can be fed directly to you as well (*see*, for example, the breadth of Google’s customization options at [www.google.com/ig/directory?hl=en](http://www.google.com/ig/directory?hl=en)). These sites carry the business theory of “mass customization” — “personalization at mass-production prices” — to another level by providing consumers the tools to personalize at no cost, other than their own time ([www.dallas-fed.org/eyi/tech/9909custom.html](http://www.dallas-fed.org/eyi/tech/9909custom.html)).

### LIVING OUTSIDE

#### OUTLOOK’S INBOX

Another way to automate your e-commerce practice is by streamlining your Outlook Inbox. It’s often been said that attorneys “live in their Inbox,” exchanging documents and messages constantly (especially since the advent of the Blackberry and similar devices). But constant use makes the Inbox quite crowded, leaving it hard to find even recent messages when they’re needed, much less such ancient history as messages from last week, or last month.

Fortunately, Outlook permits easy creation of subfolders within the Inbox, and one-click filing of messages into them. As a result, when a client calls about a matter, I can reconstruct the history with a quick search of that client’s subfolder. Searching is particularly effective, too, if paper correspondence has been scanned and electronically stored in the same database. The concept of detailed e-mail Inbox subfolders seems like common sense — even the most low-tech office has separate files in a drawer for each client and matter — yet many still store e-mail in a single Inbox, just like the “out-of-the-box” browser configuration described above.

*continued on page 10*

---

## New Kinds of e-Commerce

### ***Asset Creation, Seclusion And Money Laundering in The Virtual World: It's a Real Problem That Could Easily Get Worse***

By Sean F. Kane

As more people live in the virtual world — sometimes also called the digital or synthetic world — in one of the many so-called massively multi-player online role-playing games (MMPORGs) available online, the potential for monetary abuse and malfeasance grows.

While private gaming companies built the original virtual worlds for their subscriber base, and were controlled by designers and end-user licensing agreements (EULAs), new MMPORGs provide players with more freedoms — including the ability to create, seclude or launder wealth, a very different kind of e-commerce from that to which e-commerce pioneers are accustomed.

The likelihood of this new technology being co-opted for unscrupulous purposes is great, as historically, the same thing has happened after other technological advances, such as “property” created for a game can be misappropriated, even leading to violence (see, “Virtual Worlds And Digital Rights” in the Sept. 2005 edition of our sibling newsletter, *Internet Law & Strategy*).

#### **FROM VIRTUAL CURRENCY TO HARD CASH**

The majority of MMPORGs are designed to allow gamers to build their digital persona, or “avatar,” in the virtual society by various acts, including earning virtual currency. This happens through offering virtual goods or services to others in the digital world, much like in the real world. For years, gamers have sold digital monies,

---

**Sean F. Kane** is an entertainment attorney and a member of the New York law firm of Drakeford & Kane LLC. Reach him at 212-696-0010 or skane@drakefordkane.com.

goods or property for real-world compensation on auction sites such as eBay. Likewise, virtual entrepreneurs are maintaining successful businesses in various MMPORGs. Consider Jon Jacobs, who spent \$100,000, which comprised arguably his entire net worth at the time, to purchase a digital space station in the game Entropia Universe. Since his purchase, he's generated about \$12,000 a month in income selling residential and commercial real estate on the station, and with taxes on activities of players there. By imposing taxes, it seems that Jacobs has taken the position of a quasi-governmental agency, which in itself raises issues beyond the scope of this article. But, the grand opening of the space station nightclub “Neverdie,” and profits obtained from mining/hunting rights and property sales on the station, are expected to put Jacobs' net worth at \$1.5 million, making him the first virtual-world millionaire. Likewise, the avatar named Anshe Chung, whose real-world counterpart keeps her name secret, is known as the virtual Donald Trump. In the game *Second Life*, she charges players Linden dollars (worth about 250 to the real dollar) to rent or buy virtual homesteads. The value of her synthetic real-estate holdings is estimated at around \$250,000 in hard cash. These are just two examples of people leaving the real world, and taking permanent financial and social residence in the virtual world.

Some may question the value of virtual money if it's stuck in the digital world, but as technology advances and changes, it's no longer stuck there. When MMPORGs were developed, players were able to convert virtual dollars to hard currency only through online auction sites. Then, players were able to convert digital earnings into real cash directly through virtual-currency arbitrage-trading Web sites such as [www.GamingOpenMarket.com](http://www.GamingOpenMarket.com). With credit cards, virtual currency can be converted to hard currency at the prevailing rate, giving players a better idea of the value of their virtual assets. On May 2, the virtual world took a huge step toward becoming part of the real world when Entropia

Universe's makers introduced a plan to provide its 250,000 gamers with a real-world ATM card to instantly withdraw hard cash from their virtual-world assets. The stated conversion rate will initially be one real dollar for every 10 Project Entropia Dollars (P.E.D.s). With this announcement, it will be no more difficult to access virtual monies as real-world monies, and will likely go a long way toward Entropia Universe's stated goal of creating a “full second reality.”

#### **VIRTUAL FINANCIAL CRIMES**

Interpol defines virtual money as “money value as represented by a claim on the issuer which is stored on an electronic device and accepted as a means of payment by persons other than the issuer. Virtual money is an encrypted code representing money, in the same way that paper money is only paper bearing certain characteristics such as graphics and serial numbers.”

There are two distinct types of virtual money:

- 1. Identified virtual money.** This contains information revealing the identity of the person who originally withdrew the money from the bank. The money can be traced through the economy, by the bank or law-enforcement personnel, like credit cards.
- 2. Anonymous virtual money.** Once withdrawn from an account, it can be spent or given away without leaving a transaction trail. Using blind signatures rather than non-blind signatures creates anonymous e-money.

Virtual money is money in the real sense because it can be converted into other forms of currency. A large portion of online transactions involve debit and credit cards. An advantage and purpose of using virtual money is that it allows individuals normally excluded from e-commerce, by their economic status or other reasons, to participate. The cash-like nature of virtual money means that positive credit history or an established banking relationship isn't required. Given the definitions and descriptions above, it seems clear that virtual

*continued on page 8*

## New e-Commerce

*continued from page 7*

monies in MMPORGs will fall in the virtual-money category. And, if it can be accessed instantly, safely, and with relative ease, it's likely people will feel that cash being held in a virtual world isn't really different from cash in a brick-and-mortar, or electronic, bank. With direct deposit, electronic transfers and Internet banking, more people aren't setting foot in banks, nor requesting to see hard currency. The more the boundaries are crossed between the real financial markets and the virtual worlds, the more the games become open rather than closed, and subject to being co-opted and monitored by real-world law-enforcement (but as discussed below, that doesn't seem to pose a real threat at the moment).

Also, because virtual-world monies can be passed from person to person in any amount without reporting requirements or an e-trail, it seems to fit the definition of anonymous virtual money. That being said, there's potential for unscrupulous or illegal abuses of the virtual-monetary systems that exist in the various MMPORGs. Some of these risks are:

- Unauthorized creation, transfer or redemption of virtual money;
- Using a virtual market to mask the holder or value of virtual funds; and
- Criminal attacks on virtual-money systems, leading to loss of virtual-money value or loss of function of the virtual-money system.

### **VIRTUAL ASSET CREATION AND SECLUSION**

Estimates place gamer transactions last year in Entropia Universe alone at \$165 million, which correlates to about \$650 dollars per player. If you combine the number of transactions that occurred in Entropia Universe and other MMPORGs, the result tops \$1 billion last year alone. While that may not seem much when you average it among millions of gamers, it covers the spectrum from those who don't really participate in the virtual economy, all the way to those who drive the digital economy like the

two entrepreneurs discussed earlier. And this doesn't account for the underlying value of the intellectual property that exists in these virtual worlds that hasn't been offered for sale or otherwise monetized. The actual value of the assets in the virtual world, then, is potentially astronomical. The makers and users of these games are under no obligation to track and report to the government transactions or assets amassed or held by players. And because most assets are connected to an avatar, a synthetic-individual representation, the real-world owner of the assets is given more protection from potential discovery.

Besides the loss of potential tax revenue to a government from people creating assets or generating income in the virtual world that's not being reported, the potential for illegally secluding assets in the virtual world also exists. Since the inception of Entropia Universe and certain MMPORGs, it's been possible for players to add monies to their online accounts through credit cards and electronic-bank transfers. It's possible, then, not only to create assets the government doesn't know about, but also to move real-world assets into the virtual world where they would continue to exist, and are hidden from additional governmental view. This possibility of shielding assets or income may alone be the impetus for certain people to hide behind the persona of an avatar. Through these ownership levels, players could create and hold significant financial assets not reported or subjected to scrutiny by authorities. Combine this with the ability to access these funds at a moment's notice in the real world through an ATM card, and you have a recipe for illegal activity.

### **VIRTUAL MONEY CYBERLAUNDERING**

Traditional money-laundering involves significant physical effort. A person must conceal the existence and source of the funds, and then disguise the monies to make them appear legitimately earned. To accomplish this means the launderer must physically move hard currency while not attract-

ing unwanted attention from government agencies. Initially, this was very low-tech and might involve such acts as transporting monies out of the country to regions with less-strict banking regulations, or making multiple deposits into various accounts under the \$10,000 reporting threshold. But in 1986, the Money Laundering Control Act was enacted to further criminalize these laundering techniques. As technology advanced, however, launderers began seeking quicker and easier methods to "clean" their monies. Electronic funds transfers or wire transfers became the favored method, because they provide a swift and nearly risk-free conduit to move money between countries. But these transactions involve "identified virtual money," as discussed above, so it's possible to some extent to track the funds' source and recipient.

The great demand for efficient consumer transactions has led to electronic cash, which launderers have embraced for its potentially anonymous nature. Electronic cash, or digital money, is virtual-world replacement for hard currency and, like hard currency, once removed from an account, it can be transferred or given to any party without leaving a trail — electronic or otherwise. With such freedom of unregulated and unreported access and transfer as that being offered first by Entropia Universe's accounts, the Money Laundering Control Act will be difficult to fully enforce. Also, because Entropia Universe's accounts are likely non-FDIC insured and presumably lack federal regulation, there should be no mandatory compliance with the filing regulations in the Money Laundering Control Act of 1986.

Virtual-world gamers can buy, sell, give, and trade monies and goods, so it's possible for one virtual-world avatar to arrange a meeting with another, who may or may not be in another country, and drop off goods or monies worth significant sums of hard currency for the other party to take up. Think about it: The digital transfer of perhaps a significant sum has taken place that is not being reported to any regulatory or

*continued on page 9*

---

## New e-Commerce

*continued from page 8*

investigative agency. The person controlling the second avatar could immediately access the monies through the Entropia Universe ATM card. All of this has been done quickly and easily, resulting in one party having “virtually clean” money (pun intended) without leaving a trail for investigators. If Entropia Universe accounts, or those provided by other gaming companies that will likely follow suit, are able to continue operating outside the reach of current federal regulations, then laundering funds through an MMPORG may become the easiest method ever. To combat this, the makers of Entropia Universe claim to have vetted their ATM idea with the Swedish government, where the company is located, and that protective measures have been taken to avoid any such monetary malfeasance. But because the company hasn’t released the exact nature or extent of these steps, and hasn’t dealt with the IRS or other U.S. agency on the matter, whether or not the measures will pass muster under U.S. laws, or could otherwise be circumvented, remains open for debate.

### VIRTUAL MONETARY SYSTEM ATTACKS

Recently in South Korea, two people manipulated a virtual-world server to create virtual currency worth more than \$1 million. It raises the question of whether creating virtual

dollars, which can be converted to real-world money, is merely a computer-hacking crime, or tantamount to counterfeiting or forgery. While this act may also fall under creating virtual wealth, it demonstrates potential for attacks on the virtual-world monetary systems. As with the real world, creating counterfeit virtual money can deflate the virtual-world economy. This becomes a problem because the value of every other individual’s assets in the virtual world is lessened to some extent and can cause inflation to run rampant in the system. Also, if more monies are wrongfully inserted into a system allowing for ATM cash withdrawals than the gaming company can cover, this could cause “a run on the bank,” so to speak, which could then cause serious financial damage to the company itself, with the foreseeable consequences of other gamers’ assets to follow. It’s not a difficult scenario to imagine a technically adroit and criminally inclined individual breaking into a virtual-world server, and either creating from scratch, or just wrongfully transferring property or monies from other parties to an avatar under his or her control. As has been shown historically, money-launderers or organized-crime members are nothing if not creative in using technology or innovation to advance their schemes.

### CURRENT GOVERNMENTAL POLICING

From a discussion with a representative of the U.S. Department of Justice

Computer Crime and Intellectual Property Section, it seems that the possibility of an MMPORG being co-opted for criminal purposes hasn’t become a subject of investigation. INTERPOL, however, is obviously wary. A discussion on its Web site of virtual money includes the following: “Online games now have their own foreign exchange which lets players buy and sell different virtual currencies, just as in the real world. Criminals will undoubtedly take advantage of this.” (See, [www.interpol.int/public/TechnologyCrime/CrimePrev/VirtualMoney.asp](http://www.interpol.int/public/TechnologyCrime/CrimePrev/VirtualMoney.asp).) Given the privacy protection that the virtual world can provide an avatar, a governmental investigative agency wouldn’t have access to the identity or transactions of any individual without the cooperation of the company that developed and maintains a game. And some of these companies are based in places not amenable to fostering such cross-border investigative cooperation. Although costly to develop, it’s possible to imagine that a well-funded criminal organization might create an MMPORG for the sole purpose of masking or advancing its criminal objectives — or both.

All these hurdles may make investigation and enforcement of various current laws very difficult, if not impossible, unless more, and better, monitoring and reporting requirements are attached to the virtual world. Given the state of things, we truly have entered a “brave new world.”



---

## SOX

*continued from page 4*

service. And the SEC, the Internal Revenue Service and the Public Company Accounting Oversight Board all maintain mechanisms for receipt of anonymous reports, which can be accessed by anyone located outside the United States. Any employees located in the EU who are determined to make anonymous reports might use any of these corporate or government mechanisms. Thus, it is possible that the WP29 opinion may not have any significant effect on the quantity or

quality of anonymous whistleblowing. Only time will tell.

### CONCLUSION

The powerful historical forces that gave rise to §304 of SOX and the EU data-protection laws show no signs of diminishing. Despite calls in the United States for reform of SOX, there has been no organized effort to repeal the anonymous whistleblowing requirement under §304. EU concerns about data protection appear to be increasing in this era of global outsourcing and offshoring.

Additional rounds in the contest between SOX and WP29 over any-

mous whistleblowing should be expected. The gravity of the issues at stake suggests that both sides will not give much ground.

Until the final bell rings, compliance professionals will have their hands full reconciling the requirements of §304 with EU data-protection law.



---

## Internet Speech

continued from page 5

Traditionally, courts have not claimed jurisdiction when they cannot enforce their rules. That being the case, then, unless the owner of the foreign server from which the claimant has downloaded the offending content has financial assets in the court's jurisdiction, the court will be powerless to enforce its ruling. For example, the non-enforceability of foreign judgments that contravene the First Amendment may prevent the

enforcement of foreign rulings against U.S. defendants. This should provide strong incentive for courts to abstain from exercising jurisdiction, or applying their own defamation laws.

### APPLY PROPER JURISDICTION

Jurisdiction in Internet libel cases is a controversial issue. It is likely that common-law countries will exercise their discretion not to hear a libel action under *forum non conveniens* principles, especially when it's clear that the defendant had no reason to foresee that its statements would damage the claimant's reputation in

the forum. Although we talk about e-commerce being a global business, foreign courts understand that the Internet is primarily based in the United States, and their decisions would not be enforced here.



### LAW JOURNAL NEWSLETTERS REPRINT SERVICE

Promotional article reprints of this article or any other published by LAW JOURNAL NEWSLETTERS are available.

Call Matt Solomon at 212-545-6289 or e-mail [msolomon@alm.com](mailto:msolomon@alm.com) for a free quote.

Reprints are available in paper and PDF format.

---

## Save Time

continued from page 6

Once e-mail is categorized in subfolders, then, clicking on the column headings can quickly sort it — by date, by subject, by whether the message has an attachment or not, or by any other topic.

Another great Outlook time-saver is the ability to select custom commands to add to the preset drop-down menus. A right-click on the blank areas above the toolbars and away from the drop-down menus generates the command "Customize." With that tool, most commands in the drop-down menus — and many that are not in them — can be added to Outlook's blank, otherwise wasted, areas, again giving one-click functionality. For example, a particularly valuable tool for those who use e-mail constantly is the "undelete" command, so that a message deleted in haste, or in conjunction with another, can be quickly and easily retrieved without searching through a large "deleted" folder. (This tool must be used quickly, however, because it doesn't retrieve items after intervening deletions.)

An additional set of invaluable commands are the buttons for "move" and "copy," to allow filing of messages in the subfolders described above. "Copy" lets you put a message in several places, if it affects several matters; "move" takes it out of the Inbox, and relocates it to the specific folder selected.

### DIFFERENT HELPFUL FORMATS, GADGETS AND GIMMICKS

A tool *not* included in the standard office packages, but that's necessary for attorneys who must file pleadings online in .PDF format, is .PDF-creation software (available through many vendors). With an Explorer bar for that tool, a Web site of interest can quickly be copied and preserved, as it appears on the screen — again with one click. This feature can be helpful in litigation, to show the court and trier of fact exactly what, in fact, appeared online, and how it looked on a particular date — all inherently transient qualities in a medium built on constant change — without the need to make and store expensive printouts of a complete Web page. Without such a tool, one would have to print, successively, all pages of a Web site to preserve its image. With the .PDF creator, though, the entire Web page is saved and printed in a single file, also making it easier to circulate by e-mail.

Finally, to save time for yourself and for those with whom you work (for and against), I find it helpful to always leave my contact information, such as including it in my automatic e-mail signature. While anyone involved in online commerce certainly has access to online directories and personal address books, if not a Blackberry or cell phone, the person may not always have those resources with him or her, or access to the broadband connection to use them; the other person, too, may be traveling, have lost battery power or just

not be in a position to look up an address or number. Taking the few extra seconds to leave the contact information, even when you know the recipient already has it, isn't only common courtesy, but increases the chance of a timely reply.

Of course, these tools and tips are not the complete universe of time-savers, and readers may have better products, or different ways of providing the same efficiencies. (Please feel free to send ideas for easy time-savers in common software that are not widely used to us at [laweditor@ucwphilly.rr.com](mailto:laweditor@ucwphilly.rr.com).) Also, the specifics of the techniques I've described may also change with time, as companies update and modify their products, but similar concepts should generally be present in comparable software.

But one thing that won't change is our dependence on e-mail, and on technology to move business along more quickly. Just as the castaways never were able to get off Gilligan's Island (the Professor apparently could build anything but a boat), executives in e-commerce or their legal counsel won't be able to escape the ever-present reality of the Internet speed-driven pressure to work more — and faster. Perhaps at least the technologies we use can provide some relief to help us get work done quickly and easily enough to enjoy all the fun that life and the Internet have to offer — at home and, if we so desire, at work, when we want. It can be the key to many successes.



# e-Commerce DOCKET SHEET

## **HARD DISK IMAGING OF LICENSED SOFTWARE TO ENABLE 'BROADEST AUTHORIZED USE' IS NOT FAIR USE**

The use of hard-disk imaging to install licensed software on computers in excess of the number of paid-for licenses is not protected by fair use, even where the licensee alleged that it limited simultaneous user access to the software's functionality to the number of paid-for licenses. *Wall Data, Inc. v. Los Angeles County Sheriff's Department*, No. 03-56559, 2006 U.S. App. LEXIS 12100 (9th Cir. May 17, 2006).

The appeals court upheld the trial court's grant of summary judgment, rejecting the licensee's fair-use defense, finding that each of the four fair-use factors weighed against a fair-use finding. In particular, the appeals court noted that the use of hard-drive imaging saved the licensee the time and effort that would have been required to install each copy of the software individually, rendering the licensee's use commercial, because the unauthorized copies were made to save the expense of purchasing authorized copies.

## **TRADEMARK USE PROHIBITION AGREEMENT REQUIRES EXPLANATORY LINK**

Under a settlement agreement in which a defendant agreed not to use the plaintiff's trademark in Oklahoma, the defendant's obligation to avoid consumer confusion requires it to place an "Oklahoma" link on the first page of the Web site. *Communitycare HMO, Inc. v. Memberhealth, Inc.*, No. 06-CV-187, 2006 U.S. Dist. LEXIS 28121 (N.D. Okla. May 8, 2006).

The court granted a limited temporary restraining order enforcing an

Docket Sheet is written by **Julian S. Millstein, Edward A. Pisacreta** and **Jeffrey D. Neuburger**, partners in the New York office of Brown Raysman Millstein Felder & Steiner LLP ([www.brownraysman.com](http://www.brownraysman.com)).

agreement in which two health-care companies settled prior litigation over the right to use a trademark term on products and services related to Medicare coverage. The court ruled that the defendant, which was entitled to use the trademark term in all states other than Oklahoma, had not violated either trademark law or the settlement agreement by using the trademark term on its Web site used for marketing to the entire company. The court concluded, however, that to satisfy its obligation under the settlement agreement to take steps to avoid confusion among Oklahoma consumers, the defendant should include a specific link for Oklahoma residents on the opening page of its Web site, leading to a general explanation of the differences between the plaintiff and defendant companies.

## **CREDIT AGENCY MAY BE LIABLE UNDER FCRA FOR FAILING TO PROVIDE DATABASE ACCESS SAFEGUARDS**

A credit agency may be held liable for failing to implement adequate safeguards to ensure that customers who are given direct Internet access to databases containing consumers' personal information are not violating the Fair Credit Reporting Act. *Centuori v. Experian Information Solutions, Inc.*, No. CIV 04-013, 2006 U.S. Dist. LEXIS 30390 (D. Ariz. May 12, 2006).

The court refused to dismiss the plaintiff's complaint that the agency acted willfully or negligently, or both, in allowing a public defender's office access to his credit history for purposes that the FCRA doesn't authorize. The court concluded that a jury could reasonably find, among other breaches of the high standard set by the FCRA, that the agency acted negligently or recklessly when it implemented a system allowing customers to have direct Internet access to its database, without simultaneously bolstering its review of customer applications to screen out applicants who presented a high risk of potential FCRA violations.

## **INJUNCTION TRANSFERRING DOMAIN NAME NOT WARRANTED WHERE PLAINTIFF CAN OPERATE FROM ALTERNATE SITE**

Although the plaintiff in a domain-name dispute made a sufficient showing of trademark infringement to justify the issuance of a preliminary injunction, the removal of the disputed Web site, rather than the transfer of the disputed domain name, would maintain the status quo, pending the resolution of the dispute on the merits. *C.V. Starr & Co., Inc. v. C.V. Starr & Co., Inc.*, No. 06-2157, 2006 U.S. Dist. LEXIS 27277 (S.D. N.Y. May 9, 2006).

The dispute involved the rights to a domain name between closely affiliated business entities engaged in a dissolution of their relationship. The court noted that the plaintiff had shown that customer confusion would result from the continued operation of the "cvstarr.com" Web site by the defendant. The court also noted, however, that the plaintiff had operated, and could continue to operate, at the "cvstarrco.com" Web site, pending a resolution of the dispute on the merits. The court concluded that the removal of the Web site at the disputed domain name would maintain the status quo and avoid irreparable harm to the plaintiff.

## **ONLINE AUCTION SALE NOT COMPLETE WHEN 'FINAL HAMMER FALLS'**

An online auction sale is not complete when the auction closes when the online-auction terms required the high bidder to execute a purchase agreement subsequent to the auction to finalize the purchase. *Gossett v. HBL, LLC*, No. 2:06-123, 2006 U.S. Dist. LEXIS 30435 (D. S.C. May 11, 2006).

The court rejected the high bidder's argument that the arbitration provision included in the purchase agreement that he signed subsequent to the close of the auction was not binding,

*continued on page 12*

## Docket Sheet

continued from page 11

because the auction sales transaction was complete "upon the fall of the electronic hammer." The court ruled that the auction sale was not complete, because the online-auction terms imposed several conditions precedent to the completion of the transaction, *ie*, that the high bidder contact the seller within 24 hours, make a down payment, and sign and return sale-related paperwork, including the purchase agreement, within 24 hours of the auction closing.

### FTC SUES COMPANIES

#### ALLEGED TO USE PRETEXTING

The Federal Trade Commission (FTC) has filed federal-court complaints charging five Web-based operations that have obtained and sold consumers' confidential telephone records to third parties with violating federal law. *Federal Trade Commission v. Information Search, Inc., Accusearch, Inc., CEO Group, Inc., 77 Investigations, Inc. and Integrity Security & Investigation Services, Inc.*

According to the FTC, the defendant companies advertised on the Internet that they would obtain and sell confidential telephone records. The FTC asserts that the companies' methods of obtaining the records included "pretexting," *ie*, posing as a

customer of a telecommunications carrier to induce the carrier to disclose the confidential records.

### INSTANT MESSAGES SET LONG-ARM JURISDICTION UNDER NY STATUTE

A sophisticated institutional investor entered New York to do business within the meaning of the New York long-arm statute by initiating, negotiating and concluding a \$15 million bond transaction with a New York-based securities firm via an instant-messaging system. *Deutsche Bank Securities, Inc. v. Montana Board of Investments*, No. 71, 2006 NY Slip Op. 04338 (N.Y. June 6, 2006). The court noted that under New York CPLR 302(a)(1), personal jurisdiction may be exercised over any non-domiciliary who transacts any business within the state, even if the defendant never physically enters the state, so long as the activities of the defendant "were purposeful and there is a substantial relationship between the transaction and the claim asserted." The court found that the defendant had engaged in approximately eight substantial transactions with the same securities firm over the previous 13 months, and consequently had availed itself of the benefits of conducting business in New York and had sufficient contacts with New York to justify the exercise of jurisdiction.

### CALIFORNIA APPEALS COURT SHIELDS ONLINE PUBLISHER IN APPLE TRADE SECRET CASE

A panel of the California Court of Appeal has ruled that online publishers accused of publishing Apple Computer's protected trade secrets are entitled to the protections of the California reporter's shield law. *O'Grady v. The Superior Court of Santa Clara County*, No. H0228579 (Cal. Ct. App. 6th Dist. May 26, 2006). The appeals court ruled that two online news sites devoted to information about Apple Computer products and related subjects constitute "periodical publications" within the meaning of the shield law. The court concluded that the California Legislature intended the term to encompass Web-based publications "which differ from traditional periodicals only in their tendency, which flows directly from the advanced technology they employ, to continuously update their content." The court also ruled that subpoenas directed to the e-mail providers of the news sites were unenforceable under the Federal Stored Communications Act, 18 U.S.C. §§2701-2712, concluding that there is no implied civil discovery exception to the Act's prohibitions against service-provider disclosure of the contents of e-mail communications.

The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.

**For even FASTER service, call or fax to:**

Tel: (215) 557-2300 or (800) 999-1916  
Fax: (215) 557-2301

**On the Web at:**  
[www.ljnonline.com](http://www.ljnonline.com)

**Yes! I'd like to order LJN's e-Commerce Law & Strategy® today!**

**Now just \$315\* (regularly \$365...save \$50!)**

\*Offer valid to new subscribers only

Check Enclosed     VISA     MasterCard     Bill Me

Total Amount Due \_\_\_\_\_\*\*

Account Number \_\_\_\_\_ Exp. Date \_\_\_\_\_

Signature \_\_\_\_\_ Telephone \_\_\_\_\_

\*Please make checks payable to Law Journal Newsletters.

\*\*Customers in GA add 4% sales tax; customers in AZ add 5.6%, customers in TX add 8.25%, customers in Washington, DC add 5.75% sales tax.

Name \_\_\_\_\_

Address \_\_\_\_\_

City \_\_\_\_\_ State/Zip \_\_\_\_\_

e-mail \_\_\_\_\_



Law Journal Newsletters  
1617 JFK Blvd, Suite 1750  
Philadelphia, PA 19103-9655  
[www.ljnonline.com](http://www.ljnonline.com)

**Publisher's Guarantee! You may cancel your subscription at any time, for any reason, and receive a full refund for all unmailed issues.**