Westlaw Journal

COMPUTER & INTERNET

Litigation News and Analysis • Legislation • Regulation • Expert Commentary

VOLUME 30, ISSUE 8 / SEPTEMBER 21, 2012

WHAT'S INSIDE

COMMENTARY

Practical responses to data privacy developments in the U.S. and EU (part 1)

In the first of a two-part series, Robinson Bradshaw & Hinson attorneys John M. Conley and Robert M. Bryan discuss the Federal Trade Commission's recent report on consumer privacy issues and business data collection, retention and use, and they highlight the main points for companies operating in the United States. In part two, the attorneys discuss the European Union's draft regulation on privacy and what it means for companies that do business there.

SEE PAGE 3

REUTERS/Gary Cameron

STREAMING TV

2nd Circuit: Internet company enjoined from streaming copyrighted TV shows

A federal appeals court has upheld a preliminary injunction, granted to major television studios, local affiliates and other content creators, that prevents a Seattle-based company from streaming copyrighted television shows over the Internet.

WPIX Inc. et al. v. ivi Inc. et al., No. 11-788, 2012 WL 3645304 (2d Cir. Aug. 27, 2012).

The lower court agreed with WPIX Inc., a New York City television station, and the other plaintiffs, including ABC, NBC Universal and PBS, that streaming-television provider ivi Inc. did not qualify as a "cable system" under the Copyright Act, 17 U.S.C. § 111.

"The court's statement that video streaming companies don't qualify as 'cable companies' under the Copyright Act is significant because it means that such companies can't take advantage of pre-established licensing terms that cable companies may use under U.S. copyright law," said **James Singer**, an intellectual property attorney at **Fox Rothschild** who was not involved in the case.

Therefore, U.S. District Judge Naomi R. Buchwald of the Southern District of New York granted WPIX and the other plaintiffs a preliminary injunction. She said they would likely succeed on the merits of their copyright infringement suit and suffer irreparable harm without injunctive relief.

The Internet company appealed the judge's decision. The 2nd U.S. Circuit Court of Appeals

CONTINUED ON PAGE 14

41247081

Westlaw Journal Computer & Internet

Published since November 1983

Publisher: Mary Ellen Fox

Executive Editor: Donna M. Higgins

Production Coordinator: Tricia Gorman

Managing Editor: Robert W. McSherry

Editor: Melissa Sachs, Esq.
Melissa.Sachs@thomsonreuters.com

Managing Desk Editor: Robert W. McSherry

Senior Desk Editor: Jennifer McCreary

Desk Editor: Sydney Pendleton

Westlaw Journal Computer & Internet (ISSN 2155-5982) is published biweekly by Thomson Reuters.

Thomson Reuters
175 Strafford Avenue
Building 4, Suite 140
Wayne, PA 19087
877-595-0449
Fax: 800-220-1640
www.westlaw.com
Customer service: 800-328-4880

For more information, or to subscribe, please call 800-328-9352 or visit west.thomson.com.

How to Find Documents on Westlaw
The Westlaw number of any opinion or trial filing is listed at the bottom of each article available. The numbers are configured like this: 2009 WL 000000. Sign in to Westlaw and on the "Welcome to Westlaw" page, type the Westlaw number into the box at the top left that says "Find this document by citation" and click on "Go."

TABLE OF CONTENTS

Practical responses to data privacy developments in the U.S. and EU (part 1)

By John M. Conley, Esq., and Robert M. Bryan, Esq.
Robinson Bradshaw & Hinson

On March 26 the Federal Trade Commission released the final version of its long-awaited privacy report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers."[1] The FTC's final report renews its commitment to a self-regulatory "framework," introduced in the agency's December 2010 preliminary report,[2] that is "intended to articulate best practices for companies that collect and utilize consumer data."[3] Such practices should include "privacy by design, simplified choice [for both businesses and consumers], and greater transparency."[4]

The overall message is that the FTC will not seek a legal mandate for any particular approach to privacy but will stress general — and largely non-controversial — principles, while continuing to insist that companies live up to whatever promises they make in their announced policies.

Although the seemingly "soft" language of the final report, particularly its emphasis on recommendations rather than mandates, might be encouraging to business, it is not completely consistent with the current FTC practices. It is important to remember that the FTC operates under a *very* broad mandate.

Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices" in interstate commerce and authorizes the FTC to bring administrative enforcement proceedings against offenders.[5] The usual result is a consent decree in which the respondent agrees to change its practices and sometimes to pay a fine as well. In the privacy area, however, the FTC has been moving toward treating deviations from its "best" practices as "unfair" practices — so today's recommendations may become tomorrow's administrative law.

THE CONTENTS OF THE FRAMEWORK

The first principle of the framework — "privacy by design" — means that "companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services" and "should maintain comprehensive data management procedures throughout the life cycle of their products and services."[6]


John M. Conley (L) is of counsel at **Robinson Bradshaw & Hinson** in Charlotte and Chapel Hill, N.C., and is a professor of law at the University of North Carolina at Chapel Hill. His practice focuses on intellectual property and privacy, and he has published and spoken widely on those topics as well as the social scientific study of law and finance. He can be reached at JConley@rbh.com. **Robert M. Bryan** (R) practices with the firm in Charlotte. His practice covers a broad range of intellectual property–intensive acquisitions, joint ventures, licenses and other commercial transactions. He can be reached at BBryan@rbh.com.

More specifically, the final report calls for "reasonable" efforts in the areas of data security, collection limits, data retention and disposal practices, and data accuracy. The recommended procedures track those already required in the financial sector, including risk analysis and controls, the designation and oversight of responsible personnel, and regular re-evaluation.[7]

The second principle of the framework — "simplified consumer choice" — calls for companies to provide "easy to use" privacy choice mechanisms, usually at the point of initial data collection.[8] The final report recommends making consumer choice the default option, rather than requiring the consumer to seek it out.

At the same time, however, it stresses flexibility and excludes "commonly accepted practices" (product fulfillment, internal operations, fraud prevention, legal compliance and first-party marketing) from the specific rules about consumer choice.

However, two areas will apparently be subject to special scrutiny.[9] First, the final report "advocates the continued implementation of a universal, one-step choice mechanism for online behavioral tracking, often referred to as Do Not Track."[10] The system should be easy to use, allowing consumers to "opt out of collection of behavioral data for all purposes" other than those related to the particular interaction, such as preventing click fraud or collecting de-identified data for analysis.

Second, the final report identifies two practices that "warrant a heightened level of consent — *i.e.,* affirmative express consent": making material retroactive changes to a company's privacy representations or policy, and collecting sensitive data, defined as Social Security numbers or financial, geolocation or children's data.[11]

The third principle of the framework — transparency — is the least specific, and many of the recommendations reiterate those made in the "simplified consumer choice" section. Two areas that are highlighted are "clearer, shorter, and more standardized" privacy notices and reasonable access to consumer data, with the extent of access "proportionate to the sensitivity of the data." [12]

WILL 'RECOMMENDATIONS' TURN INTO LAW?

The obvious question for lawyers advising clients is which aspect of the final report to take more seriously: the emphasis on flexibility and voluntary compliance or the multitude of specific recommendations, which are often introduced by the word *should.* Will the FTC be a passive observer, going along with whatever business wants, or will it use its enforcement powers to try to turn its recommendations into law? Several recent developments on the privacy enforcement front suggest that the FTC will be anything but passive.

Late last year, Facebook settled FTC charges that it violated Section 5 by failing to keep numerous promises it made in its privacy policy.[13] The principal allegations involved Facebook changing its website to allow public access to information that users had designated as private and permitting broader access to user information than it had promised — for example, facilitating expanded app access, sharing information with advertisers and not shutting down deactivated accounts.

The settlement required Facebook to make some significant substantive changes in its privacy practices and to subject itself to ongoing independent audits. Then, in May, MySpace settled very similar FTC charges with an equally similar consent decree.[14]

The FTC has also been actively enforcing its powers against Google, launching a major investigation into whether the company violated an existing settlement by bypassing the default privacy settings of the Safari browser; Google has recently agreed to pay $22.5 million to settle.[15]

This investigation came on the heels of a privacy-related U.S. Department of Justice investigation into Google's use of its Street View photography vehicles to collect wireless data. That investigation was dropped without charges, but Google paid a $25,000 fine to settle a related Federal Communications Commission complaint.[16]

Significantly, the FTC has not limited itself to big and obvious targets. On June 7 the FTC announced proposed consent agreements with a Georgia Toyota dealership and a Utah debt- collection agency for "allowing peer-to-peer file-sharing software to be installed on their corporate computer systems" and thus exposing consumer financial information to "viewing or downloading by any computer user with access" to the P2P network.[17]

In the car dealership case, as many as 95,000 consumer files were exposed on the P2P network, though the dealer denied — and the FTC did not contend — that any credit profiles were actually misappropriated. The FTC charged the dealer with violating Section 5 as well as the financial institution regulations that apply to it because it provides customer financing.

Despite the business-friendly tone of the final report, the message of these and several other cases brought against smaller targets is that the FTC remains a vigilant watchdog. It is important to note that in the car dealer case, the alleged violations involved not only the dealer's failure to live up to the terms of its own privacy policy, but its failure to adopt reasonable data security measures in the first place by allowing the installation of the P2P software.

When the FTC acts under the broad mandate of Section 5, as opposed to the more specific enforcement powers given by various financial statutes, the agency usually focuses on *procedure* — that is, whether a company keeps whatever privacy promises it makes. Its attention, however, is typically triggered by the *substance* of the target's behavior, in particular, whether and how it shares consumer data with third parties. The message for companies that collect consumer data seems to be that simply not violating your own policy is not enough — the FTC is increasingly asking whether that policy offers sufficient protection.

> The FTC has been moving toward treating deviations from its "best" practices as "unfair" practices — so today's recommendations may become tomorrow's administrative law.

Consistent with this growing attention to substance, even the final report endorses one piece of new legislation to regulate "data brokers."[18] Although the final report offers no definition of this term, it is generally understood to cover all entities that collect and sell consumer information, including credit bureaus, catalog sellers, ad networks and various kinds of Internet analytics companies. The FTC recommends that these entities be required to identify themselves and their practices to consumers and to detail the access rights to the data they collect and other choices that they provide.

The FTC final report presents — at least on the surface — a flexible "framework" approach, promoting recommendations rather than regulations and urging a collaborative effort to develop best practices that will protect privacy while balancing the legitimate needs of businesses and consumers.

But the FTC's recent enforcement efforts have sent a somewhat contradictory message. It has targeted both large (Google) and small (a Georgia car dealer) businesses. Moreover, the FTC seems to be moving beyond its traditional practice of policing companies' compliance with their own privacy policies and toward the creation and enforcement of minimum substantive standards.

ADAPTING THIS FRAMEWORK TO U.S. BUSINESSES

What should companies expect from the FTC?

Companies should give more credence to the FTC's actions — its enforcement activities — than to the generally conciliatory tone of the final report.[19] It used to be possible to advise companies that any privacy policy would suffice as long as the company did what it promised. Now, however, the FTC's message seems to be that mere compliance is not enough and that the policies themselves must offer "reasonable" privacy protection to consumers.

What kinds of protection will the FTC be looking for?

The best clues to what the FTC considers "reasonable" probably lie in the final report. The prudent assumption is that many of the "recommendations" of the final report will become law indirectly, through the vehicle of Section 5 enforcement actions.

Although the FTC's report emphasizes data security, collection limits, retention and disposal practices, and accuracy, the agency is unlikely to develop detailed top-down standards for any of these and is more likely to rely on enforcing evolving industry-developed best practices.

The final report stresses the need to offer simplified consumer choices about privacy at the point of initial data collection. It also advises companies to make sure they obtain express affirmative consent to material changes in their privacy policies and to any collection of sensitive data, defined as Social Security numbers or financial, geolocation or children's data. Finally, the entire data collection and analysis industry is urged to develop a universal, one-step Do Not Track mechanism.

Will the FTC target particular sectors?

Since its inception, American privacy law has focused primarily on identity theft and its financial implications. Under the Gramm-Leach-Bliley Act[20] and the Fair and Accurate Credit Transactions Act,[21] the FTC already has specific authority over a wide range of companies that extend credit or engage in other non-banking financial activities. As the auto-dealer case illustrates, the FTC is developing experience in asserting that authority.

Together with the inclusion of financial data in the final report's "sensitive data" category, the only logical inference is that companies that collect and/or hold consumer financial information will be at least one of the primary targets for future enforcement activities. Of the other categories of sensitive data, geolocation data and data collected by mobile apps have appeared on the FTC's recent radar.[22] Social Security numbers and children's data are already heavily regulated by, respectively, state privacy laws and the federal Children's Online Privacy Protection Act.[23]

Are there models to follow in designing policies that will satisfy the FTC?

It seems likely that the FTC will focus both on data security and use. With respect to data security, multiple detailed industry-specific guidelines are already available. The best guide for data use may be a set of detailed rules that the FTC has already developed for financial data: the Financial Privacy Rule and the Safeguards Rule promulgated under Gramm-Leach-Bliley, and the FACTA Red Flags Rule.[24]

The collective principles of compliance include:

- Providing consumers with a clear and conspicuous privacy policy.
- Requiring affirmative opt-out before transferring data to third parties.
- Designing, implementing and monitoring a written data security plan.
- Implementing a comparable program for detecting and acting on suspicious anomalies, or "red flags."

There are several collective principles of compliance (see box).

While these are essential elements of compliance for companies dealing with financial data, they are also an excellent starting point for any company. By adapting the relevant principles to their own business contexts, other kinds of companies will likely satisfy the FTC, ensure that they are in compliance with most state privacy laws and — as a bonus — have made an excellent start on compliance in the European Union, which will be the focus of the second part of this series. WJ

NOTES

1 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, 2012 WL 1034528 (Mar. 26, 2012).

2 *See id.* at i-iii.

3 *Id.* at iii.

4 *Id.*

5 15 U.S.C. § 45.

6 FTC report at vii.

7 *See, e.g.,* Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. 106–102, 113 Stat 1338 (1999), 12 U.S.C.A. § 1811; Fair and Accurate Credit Transactions Act, Pub. L. 108-159, 117 Stat. 1952 (2003), 15 U.S.C.A. § 1601.

8 FTC report at 35.

9 In an additional nod in the direction of business-friendliness, the FTC specifically recommends that companies that collect only non-sensitive data from fewer than 5,000 consumers per year be excluded from the framework (versus near-universal coverage in the preliminary report).

10 FTC report at 52.

11 *Id.* at 57.

12 *Id.* at 64-71.

13 Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 20110), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm.

14 *In the Matter of MySpace LLC,* 2012 WL 1745313 (F.T.C. May 8, 1012).

15 Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* http://www.ftc.gov/opa/2012/08/google.shtm.

16 *In the Matter of Google Inc.,* 2012 WL 1305318 (F.T.C. Apr. 13, 2012).

17 Press Release, Fed. Trade Comm'n, FTC Charges Businesses Exposed Sensitive Information on Peer-to-Peer File-Sharing Networks, Putting Thousands of Consumers at Risk (June 7, 2012), *available at* http://www.ftc.gov/opa/2012/06/epn-franklin.shtm; *In the Matter of Franklin's Budget Car Sales, Inc.,* 2012 WL 2150214 (F.T.C. June 7, 2012); *In the Matter of EPN Inc.,* 2012 WL 2150217 (F.T.C. June 7, 2012).

18 *See* FTC report at 14.

19 Fed. Trade Comm'n, Commission Actions for September 2012, http://www.ftc.gov/os/actions.shtm.

20 Gramm-Leach-Bliley, Pub. L. 106–102.

21 Fair and Accurate Credit Transactions Act, Pub. L. 108-159.

22 *See* Fed. Trade Comm'n, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (February 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; Commission Actions for September 2012, *supra* note 19.

23 Children's Online Privacy Protection Act of 1998, Pub. L. 105–277, 112 Stat. 2681–728 (1998), 15 U.S.C.A. § 6501.

24 Fed. Trade Comm'n, Privacy of Consumer Financial Information (Privacy Rule), 16 C.F.R. § 313 (2000); Standards for Safeguarding Customer Information (Safeguards Rule), 16 C.F.R. § 314 (2002).

E-BOOKS

3 publishers settle feds' e-book antitrust suit

HarperCollins, Simon & Schuster and Hachette Book Group have received court approval to settle the government's charges that they colluded to raise e-book prices.

United States v. Apple Inc. et al., No. 12 Civ. 2826, 2012 WL 3865135 (S.D.N.Y. Sept. 5, 2012).

U.S. District Judge Denise Cote of the Southern District of New York granted the government's motion to enter the settlement as a final judgment Sept. 5.

A week earlier, the three publishers agreed to pay $69 million to resolve a lawsuit filed by 49 states over the same alleged price-fixing scheme.

In the federal government's case, however, the companies will not have to pay any fines or restitution, but they agreed to change some business practices.

Judge Cote said in her order that the settlement "properly restricts defendants' activities … with an eye to ending the price-fixing and preventing its recurrence."

Therefore, the consent decree met the standards set forth in the Tunney Act, 15 U.S.C. § 16(e)(1), which requires courts to analyze whether a proposed settlement in a civil antitrust suit with the government is "in the public interest," the judge concluded.

Hillel I. Parness, a partner at **Robins, Kaplan, Miller & Ciresi** in New York, commented on the judge's ruling.

"Throughout the opinion, the court reiterated the theme that based on the allegations of contractual price-fixing, the settlement's focus on unwinding those contracts and prohibiting future contracts for various time periods was appropriate," he said.

Parness advises clients on Internet and intellectual property issues. He was not involved in the case.

"The immediate impact of the decision remains to be seen," Parness said, "as there are other non-settling defendants … indicating they intend to fight on and appeal this ruling."

REUTERS/Shannon Stapleton

The defendants allegedly conspired to raise e-book prices because they were concerned Amazon's discount pricing strategy would eat into their profits. Amazon's Kindle Fire book reader is shown here.

THE ANTITRUST CHARGES

The Justice Department sued Apple and five publishers, including Hachette, HarperCollins and Simon & Schuster, in April.

The government alleged the publishers conspired to raise e-book prices and restrain trade through unlawful agreements with Apple in violation of Section 1 of the Sherman Antitrust Act, 15 U.S.C. § 1.

The CEOs of each company started meeting around September 2008 to discuss online retailers' pricing strategies for e-books, the complaint said. The publishers allegedly feared discounting e-books would eat into their profit margins, especially for hardcover new releases and bestsellers.

In late 2009, Apple announced the upcoming launch of the iPad tablet device and was deciding whether to open an online store to sell e-books, the complaint said.

The publishers began talking about pricing strategies with Apple, given their common motivation to limit e-book retail price competition, the suit said.

Allegedly, through these meetings, Apple and the five publishers agreed to switch from a "wholesale" pricing model to an "agency" pricing model to combat the discount pricing strategy favored by online retail giant Amazon.

Under the new pricing model, rather than selling e-books at a wholesale or discount price to retailers such as Apple or Amazon, the retailers would serve as the publishers' "agents" and receive a percentage of each sale, the complaint alleged.

Additionally, the publishers agreed to include "most favored nation" clauses in their contracts with Apple, which purportedly guaranteed that Apple's iBookstore could offer e-books at the lowest prices, the suit said.

THE SETTLEMENT

According to Judge Cote's order, the settlement bars Hachette, HarperCollins and Simon & Schuster from entering into unlawful agreements with the intent to raise e-book prices and restrain trade.

It also prohibits them from implementing an agency pricing model for two years, a switch that Apple allegedly encouraged to limit retail price competition, and from using "most favored nation" clauses in their contracts for five years, the order says.

"The immediate impact of the decision remains to be seen, as there are other non-settling defendants ... indicating they intend to fight on and appeal this ruling," said Hillel I. Parness, a partner at Robins, Kaplan, Miller & Ciresi.

Although Judge Cote found the proposed final settlement was in the public interest, it received an overwhelming number of negative public comments opposing the deal, the order says.

Many comments suggested that the settlement was overbroad and would harm brick-and-mortar bookstores, according to the order.

In response, the judge said the complaint seeks to redress injuries to e-book consumers, not other third-party industry stakeholders.

"It is not the place of the court to protect these bookstores and other stakeholders from the vicissitudes of a competitive market," Judge Cote wrote. "What is clear, however, is the need for industry players to play by the antitrust rules when confronted with new market forces." WJ

Attorneys:
Plaintiff: Mark W. Ryan, Stephanie A. Fleming, Lawrence E. Buterman and Laura B. Collins, U.S. Department of Justice, Antitrust Division, Washington

Defendant (Hachette): Walter B. Stuart IV and Samuel J. Rubin, Freshfields Bruckhaus Deringer LLP, New York

Defendant (HarperCollins): Shepard Goldfein, Clifford H. Aronson and Paul M. Eckles, Skadden, Arps, Slate, Meagher & Flom, New York

Defendant (Simon & Schuster): Helene D. Jaffe and Jennifer R. Scullion, Proskauer Rose LLP, New York; James W. Quinn and Yehudah L. Buchweitz, Weil, Gotshal & Manges, New York

Related Court Document:
Opinion and order: 2012 WL 3865135

See Document Section B (P. 29) for the opinion and order.

Lexmark must face cartridge supplier's false-advertising claims

A toner cartridge supplier may pursue its false-advertising and unfair-competition claims against Lexmark International based on the printer manufacturer's alleged misrepresentations to customers that the supplier in unlawful conduct and sold infringing products, a federal appeals court has ruled.

Static Control Components Inc. v. Lexmark International Inc., Nos. 09-6287, 09-6288 and 09-6449, 2012 WL 3765010 (6th Cir. Aug. 29, 2012).

Static Control Components Inc., which supplies remanufactured toner cartridges, alleged that Lexmark's false statements harmed its business reputation, the 6th U.S. Circuit Court of Appeals' opinion said.

Therefore, under the court's precedent, the panel ruled that Static Control had standing to pursue its claims for violations of the Lanham Act, 15 U.S.C. § 1125(a), and related state law unfair-competition charges.

CLAIMS AND COUNTERCLAIMS

Writing for the panel, Judge Karen N. Moore explained the complex procedural history of the case and the technology involved.

Lexmark sells laser printers and corresponding toner cartridges that contain microchips. Its printers will reject any toner cartridges that lack the microchip.

Static Control figured out how to replicate the microchips for toner cartridges, the opinion says. It began to sell them to remanufacturers, which refill used Lexmark toner cartridges and resell them at a lower price.

Lexmark sued Static Control in the U.S. District Court for the Eastern District of Kentucky in 2002.

The suit alleged that Static Control copied Lexmark's source code when it duplicated the microchips and circumvented technology security measures, violating the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2)(A).

In 2003 the District Court granted Lexmark a preliminary injunction.

While the DMCA suit was pending, Static Control redesigned its microchips and sued Lexmark in the U.S. District Court for the Middle District of North Carolina, requesting a declaratory judgment that its new microchips did not infringe any copyrights.

It also alleged that Lexmark restrained trade in the printing cartridge market, violating federal antitrust laws, and engaged in false advertising and unfair competition under the Lanham Act and North Carolina's unfair- and deceptive-trade-practices statute, N.C. Gen. Stat. § 75-1.

The two suits were consolidated in the Eastern District of Kentucky in 2004, and Static Control appealed the injunction to the 6th Circuit.

In a 2-1 opinion, the appellate panel reversed the injunction, rejecting Lexmark's copyright infringement theories.

The panel sent the case back to the District Court, which then dismissed Static Control's antitrust, false-advertising and unfair-competition claims, finding that the supplier lacked standing to pursue them.

Both parties appealed again to the 6th Circuit.

STANDING

On appeal, the main issues presented concerned whether Static Control had standing to pursue its antitrust, false-advertising and unfair-competition claims.

While the three-judge panel agreed with Lexmark that Static Control did not have standing to pursue its antitrust allegations, it disagreed with the printer manufacturer about Static Control's standing to move forward with its false-advertising and unfair-competition allegations.

REUTERS/Steve Marcus

Lexmark's toner cartridges contain microchips so its printers can reject any cartridge that does not contain the chip. A Lexmark Platinum Pro905 printer is shown here.

Lexmark had argued that Static Control had no standing because the two companies were not in direct competition, a factor that other circuit courts have required for false-advertising claims.

The panel, however, said that it must follow *Frisch's Restaurants v. Elby's Big Boy of Steubenville*, 670 F.2d 642, 649-50 (6th Cir. 1982), which only required Static Control to show a "likelihood of injury and causation."

"Even if we were to prefer the approach taken by our sister circuits, we cannot overturn a prior published decision of this court absent inconsistent Supreme Court precedent or an *en banc* reversal," the appeals court said.

The panel sent the remaining issues back to the District Court. WJ

Attorneys:
Appellant/cross-appellee: Seth D. Greenstein, Constantine & Cannon, Washington

Appellee/cross-appellant: Steven B. Loy, Stoll Keenon Ogden PLLC, Lexington, Ky.

Related Court Document:
Opinion: 2012 WL 3765010

Appeals court reinstates damages award in music piracy case

(Reuters) - The music industry has won the latest round in its long-running legal battle against a woman accused of illegally downloading and sharing two dozen songs on the Kazaa peer-to-peer network.

Capitol Records Inc. et al. v. Thomas-Rasset, No. 11-2820, 2012 WL 3930988 (8th Cir. Sept. 11, 2012).

The 8th U.S. Circuit Court of Appeals in St. Paul, Minn., reinstated a $222,000 jury verdict against Jammie Thomas-Rasset, rejecting her arguments that the damages award was excessive and violated her due process rights under the U.S. Constitution.

The decision is the latest to address the music industry's ability to use the Copyright Act, 17 U.S.C. § 101, to pursue individuals who illegally download music from the Internet. The law allows copyright owners to recover damages between $750 and $150,000 per infringed work.

Thomas-Rasset, from Brainerd, Minn., was one of 18,000 individuals sued by the Recording Industry Association of America between 2003 and 2008 in a legal assault meant to discourage people from illegally downloading songs from sites like Kazaa.

The industry organization accused her of illegally downloading more than 1,700 files. After failing to reach a settlement, the association sued Thomas-Rasset in 2006 over 24 songs on behalf of six major record labels, including Sony BMG Music Entertainment, UMG Recordings Inc. and Arista Records.

The case has followed a circuitous path. Thomas-Rasset lost her first trial in 2007 and was ordered to pay $222,000, only to have the court throw out the verdict because of a faulty jury instruction.

At her second trial, Thomas-Rasset testified that her ex-boyfriend or sons, then 8 and 10, were most likely responsible for downloading and distributing the songs. The jury awarded the record labels $1.92 million in damages. But the court lowered the damages to $54,000, calling the jury's award "shocking." Instead of accepting the lowered amount, the record companies exercised their right to a new trial, and a third jury awarded the music industry $1.5 million in damages. The trial court again ruled that the maximum amount allowed by due process was only $54,000.

> The $222,000 award, equivalent to $9,250 per song, was at the lower end of the $750 to $150,000 range that Congress established, the panel noted.

The recording companies appealed.

On Sept. 11, a unanimous three-judge panel of the 8th Circuit reinstated the original $222,000 in damages that the first jury had awarded.

The $222,000 award was not "so severe and oppressive" as to violate the Constitution, Judge Steven Colloton wrote for the panel. Rather, the amount, equivalent to $9,250 per song, was at the lower end of the $750 to $150,000 range that Congress established.

Thomas-Rasset argued that if the labels had sued her over 1,000 songs, the damages would be clearly excessive at over $9 million. But the panel refused to extrapolate.

"If and when a jury returns a multimillion-dollar award for noncommercial online copyright infringement, then there will be time enough to consider it," Judge Colloton wrote.

Kiwi Camara, a lawyer for Thomas-Rasset, called the $222,000 damages award "punitive" and out of line with the U.S. Supreme Court's rulings. He said he would likely appeal the case to the high court.

The Recording Industry Association of America welcomed the court's decision. We "look forward to putting this case behind us," the organization said in a statement. The group has ended its lawsuit campaign and now sends warning notices to users caught illegally downloading music.

In a separate case in 2011, the 1st Circuit reinstated a $675,000 judgment against Joel Tenenbaum, a former Boston University student, for 30 charges of illegal downloading. That ruling reversed a trial judge's decision to knock the award down to $67,500.

Tenenbaum appealed that case to the Supreme Court, arguing that the Copyright Act was never meant to be applied to individual consumers. But the Supreme Court declined to hear the case in May, allowing the 1st Circuit decision to stand. WJ

(Reporting by Terry Baynes; editing by Tim Dobbyn)

Attorneys:
Plaintiffs-appellants: Felicia Boyd, Barnes & Thornburg, Minneapolis

Defendant-appellee: Kiwi A.D. Camara, Joe Sibley and Michael L. Wilson, Camara & Sibley, Houston

Related Court Document:
Opinion: 2012 WL 3930988

See Document Section C (P. 41) for the opinion.

SCAREWARE

PC users say Avanquest markets scam antivirus software

Software designer Avanquest is facing a lawsuit accusing it of defrauding consumers by selling them "scareware" that falsely claims their computers have been infected by a virus.

Worley v. Avanquest North America Inc., No. 3:12-cv-04391, complaint filed (N.D. Cal., S.F. Div. Aug. 21, 2012).

The company makes a pair of software products, Fix-It Utilities and System Suite PC Tune-Up & Repair, that it says detect and repair privacy threats, harmful errors, viruses and other PC security risks.

The products also are marketed to increase system startup speeds and optimize a PC's performance, according to the proposed class action filed by Benson Worley in the U.S. District Court for the Northern District of California.

"In reality, Avanquest's descriptions of the scareware's utility serve as the initial phase of a fraudulent scheme to induce consumers into purchasing its products, and then to convince them into paying ongoing subscription fees to continue using the software," the lawsuit says.

After consumers install the software, they are encouraged to conduct a "diagnostic scan" to assess the condition of the PC, according to the suit.

The software reports, "in ominous fashion, that harmful problems are lowering the PC's condition," the suit continues. The consumers are then offered the chance to "fix" the PC by removing purported errors listed by Avanquest's products, the complaint says.

But the suit alleges the diagnostic testing procedure does not perform a credible evaluation of the PC.

"Instead, Avanquest intentionally designed the scareware to always report that a user's PC needs repair and is afflicted with harmful errors, privacy risks and other problems — regardless of its actual state," the complaint says.

> "Avanquest's descriptions of the scareware's utility serve as the initial phase of a fraudulent scheme to induce consumers into purchasing its products," the suit says.

As a result, consumers are tricked into believing that the software is reporting and repairing actual errors, according to the suit. Because the same process is repeated each time consumers run the software, they are fraudulently induced into continually renewing their subscriptions, the complaint says.

The suit seeks damages and injunctive relief for breach of contract, breach of warranty, fraudulent inducement and violations of California's unfair-competition law, Cal. Bus. & Prof. Code § 17200. WJ

Attorney:
Plaintiff: Sean P. Reis, Edelson McGuire LLP, Rancho Santa Margarita, Calif.

Related Court Document:
Complaint: 2012 WL 3642843

U.S. is using proprietary mailing software without permission, tech firm says

A technology company says in a lawsuit that the Postal Service is using its specialized package delivery software without permission.

RQ Squared LLC v. United States, No. 12-CV-527, complaint filed (Fed. Cl. Aug. 21, 2012).

Plaintiff RQ Squared says the United States has misappropriated its trade secrets for a software product that allows businesses to assist customers with product returns. The company also claims the Postal Service has breached an implied-in-fact agreement to refrain from making independent commercial use of the technology.

In the complaint pending in the U.S. Court of Federal Claims, the plaintiff says it developed a proprietary Web-based program and software called the "dual label system."

> The suit alleges the United States misappropriated trade secrets for a software product that allows businesses to assist customers with product returns.

REUTERS/Shannon Stapleton

The system involves the use of mailing labels that have multiple bar codes that allow a package to be shipped back to a merchant by the Postal Service and a private carrier, with each entity handling the item for part of the journey, the complaint says.

RQ Squared says its system, which allows packages to be tracked along the route, increases delivery efficiency when consumers are returning merchandise. The company says it began working with Postal Service representatives in 2005 to submit an application to become an approved vendor.

RQ Squared gave the government information about the software system so the Postal Service could assess the feasibility of using the technology, and the government and the plaintiff reached an implied-in-fact agreement that the technological information would be confidential and proprietary to RQ Squared, according to the complaint.

The company claims that RQ's written communications with the Postal Service, including emails and federal forms, confirmed that the information on dual label system was proprietary. The plaintiff also asserts it negotiated with the Postal Service about using the software in a package delivery relationship with nonparty Federal Express.

The suit says the Postal Service abruptly stopped communicating with RQ in mid-2007, and in February 2009 started a program that would allow people to return packages to merchants.

The Postal Service's program duplicates the plaintiff's proprietary dual label system and would not have been possible without the misappropriation of RQ Squared's technology, the complaint alleges.

In addition, the government is using the plaintiff's duplicate system with Federal Express and nonparty United Parcel Service, the suit says.

The plaintiff says the Postal Service disclosed the proprietary information to both carriers in breach of its confidentiality obligations.

RQ is seeking unspecified damages, interest, costs and attorney fees.

At press time, the government had not filed a response to the suit. WJ

Attorney:
Plaintiff: Brian C. Duffy, Duffy & Young, Charleston, N.C.

Related Court Document:
Complaint: 2012 WL 3869848

Fry's, software maker sell defective voice-recognition software, suit says

Fry's Electronics Inc. and a software products developer are facing a class-action lawsuit for allegedly misleading a consumer into buying a voice-recognition software package that does not work.

Nathan v. Fry's Electronics Inc., BC491300, complaint filed (Cal. Super. Ct., L.A. County Aug. 31, 2012).

Michael Nathan alleges that Nuance Communication Inc. falsely claims that its Dragon Speaking software recognizes speech with "99 percent accuracy."

Instead, the software does not perform "any credible evaluation of a consumer's speech and accent," Nathan says in his complaint filed in the Los Angeles County Superior Court.

The plaintiff says he purchased the software from a Fry's store in California because his job requires him to read and type pages of material on a daily basis.

At the time of purchase, a store employee, "acting like he was the creator of the Dragon," allegedly told Nathan that the software package would make his "life a lot easier" and that he could return the $249.99 software for a refund if he were not satisfied.

But after Nathan installed the product on his computer, he spent more than two weeks at three to five hours a day reading materials and articles to enable the software to recognize his speech and accent "at no avail," the suit says.

When he decided to return the product, a store supervisor allegedly told him it was against federal law to accept open software.

The complaint adds that Nuance does not offer a refund and it recommends that users return the software to the place of purchase even though it knows "it would not be returnable."

Nathan seeks damages for breach of warranty, false advertising, fraudulent inducement, breach contract and unfair competition. WJ

Attorneys:
Plaintiff: Motaz M. Gerges and Andrew L. Levin, Law Office of Motaz M. Gerges, Sherman, Calif.

Related Court Document:
Complaint: 2012 WL 3875610

Courtesy of nuance.com

The plaintiff alleges that Nuance Communication Inc. falsely claims that its Dragon Speaking software recognizes speech with "99 percent accuracy."

TSA to face claims over missing electronics

A South Carolina man may go forward with some of his claims that $2,300 worth of electronic gear disappeared from his luggage while it was in the hands of federal Transportation Security Administration officers.

Williams v. United States, No. 11-02316, 2012 WL 3638788 (D.S.C. Aug. 22, 2012).

U.S. District Judge R. Bryan Harwell of the District of South Carolina dismissed plaintiff Reynolds Williams' claim for conversion against the TSA but declined to dismiss bailment and negligence claims against the agency.

Williams was flying home to Florence, S.C., from O'Hare Airport in Chicago May 18, 2011, when he checked a bag containing a laptop computer, an e-book reader and related accessories, the judge's order says. He claims he handed his bag to a uniformed TSA officer at the US Air counter.

The judge urged the parties to come to a resolution of the matter without taking up any more of the court's time.

When Williams arrived home later that day and retrieved his bag from the baggage conveyor belt, he discovered that all of his electronic equipment was missing and replaced with a TSA notice that the bag had been opened, according to the order.

Williams sued the federal government, alleging bailment, negligence and conversion. The suit does not include any claims against the airline.

A magistrate judge recommended that the court grant the government's motion to dismiss the case. Williams objected only to dismissal of the bailment and negligence claims.

CONVERSION CLAIM NOT VIABLE

Ruling on the magistrate's recommendations, Judge Harwell dismissed the conversion charge because the TSA is protected by sovereign immunity for actions committed by its employees outside the scope of their employment.

REUTERS/Sue Ogrocki

Even accepting Williams' allegation that a TSA employee stole his equipment, such a theft would be outside the scope of the worker's employment, and, since the TSA did not waive sovereign immunity, it cannot be held liable under the Federal Tort Claims Act, the judge said.

BAILMENT AND NEGLIGENCE

Under Illinois law, which applies to occurrences at O'Hare Airport, bailment refers to the relationship between two parties when one transfers the custody of goods to another. Such a relationship confers an obligation on the recipient to protect and preserve the goods entrusted to it, Judge Harwell explained.

Although Williams alleges that both TSA and US Air had possession of his luggage at different times, the court could infer from Williams' complaint that he has sufficiently alleged that the TSA did have exclusive custody for a period of time and that his electronic devices went missing during that "window of exclusive control," Judge Harwell said.

If the bailment claim survives dismissal, Williams argued, the negligence claim should also survive because if the electronics went missing while in the TSA's control, there is a presumption of negligence on the part of the agency for failing to protect his property.

Judge Harwell agreed. He noted that if Williams does not prevail on his negligence claim, he could alternatively plead a breach-of-contract theory based on the TSA's failure to safeguard his property.

Williams cannot, however, plead both negligence and breach of contract at the same time, the judge said.

While Judge Harwell denied the government's motion to dismiss the bailment and negligence claims, he urged the parties to come to a resolution of the matter without incurring any further legal costs or taking up any more of the court's time.

He said in a footnote that the parties have already generated 28 docket entries and filed more than 70 pages of pleadings and are likely to rack up future expenses far exceeding the $2,300 in controversy. WJ

Attorneys:
Plaintiff: Reynolds Williams, *pro se,* Willcox, Buyck & Williams, Florence, S.C.

Defendant: Christie V. Newman, U.S. attorney's office, Columbia, S.C.

Related Court Document:
Order: 2012 WL 3638788

Streaming TV

CONTINUED FROM PAGE 1

found that Judge Buchwald did not abuse her discretion and the panel upheld the preliminary injunction.

Under the court's reasoning, Singer said, "if a video streaming website wants to retransmit a live broadcast signal, it must first negotiate a license with the broadcaster."

According to the panel's opinion, the major television networks, studios and other content creators had not consented nor allowed ivi to stream their protected content over the Internet.

When the streaming service launched in September 2010, they sent cease-and-desist letters to the company, the opinion says.

In response to the letters, ivi argued that it qualified as a "cable system" under federal copyright law and, therefore, was entitled to a compulsory license from the broadcasters to continue retransmitting the copyrighted programming.

The plaintiffs then sued ivi for copyright infringement, seeking damages and injunctive relief.

Judge Buchwald granted the plaintiffs' motion for a preliminary injunction.

On appeal, the 2nd Circuit panel reviewed the decision for an abuse of discretion, but found none.

"It is undisputed that the plaintiffs owned valid copyrights to the television programming that ivi publicly performed without plaintiffs' consent," Circuit Judge Denny Chin wrote for the panel.

Therefore, ivi would only have a defense if it qualifies as a "cable system" under federal copyright law, which would entitle it to a compulsory license.

To determine whether the Copyright Act extended compulsory licenses to Internet retransmissions, Judge Chin applied the two-step test outlined in *Chevron USA v. Natural Resources Defense Council*, 467 U.S. 837 (1984). Under the first part of the test, the appeals court attempted to derive Congress' intent in enacting the Copyright Act through the law's text and legislative history.

"The court's statement that video streaming companies don't qualify as 'cable companies' under the Copyright Act is significant because it means that such companies can't take advantage of pre-established licensing terms that cable companies may use under U.S. copyright law," said James Singer, an intellectual property attorney at Fox Rothschild.

Judge Chin said the statutory text did not clearly indicate whether a service that streams live television programming over the Internet qualifies as a "cable system."

The legislative history, however, showed that Congress enacted the compulsory license to help bring television programming to remote locations.

With the compulsory license, the copyright owners still had the incentive to produce protected content but remote cable systems did not have the high costs of negotiating individual licenses, Judge Chin explained.

On the other hand, he wrote, "Internet retransmission services are not seeking to address issues of reception and remote access to over-the-air television signals."

Therefore, Congress clearly did not intend for the compulsory license to extend to Internet transmissions, Judge Chin said.

Moreover, *Chevron*'s second step — analyzing the Copyright Office's interpretation of the statute — confirms that conclusion, the panel pointed out.

"The Copyright Office has consistently concluded that Internet retransmission services are not cable systems and do not qualify for … compulsory licenses," Judge Chin wrote.

The panel, therefore, agreed with the lower court that the major networks would likely succeed on the merits of their case and would suffer irreparable harm without a preliminary injunction.

Additionally, the panel said, the balance of hardships and public interest factors weighed in favor of granting the preliminary injunction. WJ

Attorneys:
Plaintiffs-appellees: Robert A. Garrett, Hadrian R. Katz, Lisa S. Blatt, C. Scott Morrow and R. Reeves Anderson, Arnold & Porter, Washington; Peter L. Zimroth, Arnold & Porter, New York

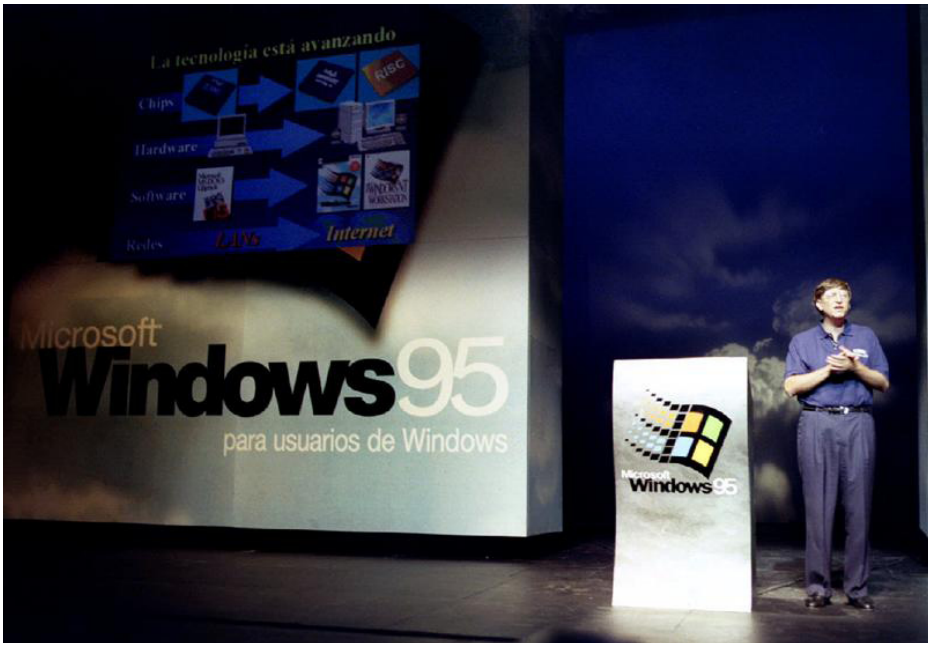
Defendants-appellants: Lawrence D. Graham and Ellen M. Bierman, Black Lowe & Graham, Seattle

Related Court Document:
Opinion: 2012 WL 3645304

See Document Section A (P. 19) for the opinion.

Novell to ask 10th Circuit to revive $1 billion antitrust suit against Microsoft

Novell Inc. will try to revive its eight-year-old lawsuit alleging Microsoft Corp. withheld key technical information that would have made Novell's WordPerfect and Quattro Pro software compatible with the Windows 95 operating system.



REUTERS Desmond Boylan

Bill Gates announces the launch of Windows 95 to customers in Spain in September 1995. Novell claimed Microsoft intentionally withheld application programming interfaces for Windows 95 before launching the operating system.

Novell Inc. v. Microsoft Corp., No. 12-4143, notice of appeal filed (10th Cir. Aug. 10, 2012).

In a lawsuit filed in Utah federal court, Novell alleged Microsoft withheld the critical information in order to thwart competition in violation of the Sherman Act, 15 U.S.C §§ 1-2.

U.S. District Judge J. Frederick Motz threw out the case in July, ruling that Novell lacked sufficient evidence to prove that Microsoft monopolized the market for software applications and operating systems. *Novell Inc. v. Microsoft Corp.*, No. 04-1045, 2012 WL 2913234 (D. Utah July 16, 2012).

Novell filed a notice of appeal with the 10th U.S. Circuit Court of Appeals Aug. 10. The company will have 40 days to file an opening brief once the district clerk notifies the parties and the court that the record is complete for purposes of appeal, according to the court docket.

Novell claimed Microsoft intentionally withheld application programming interfaces for Windows 95 before launching the operating system.

An API is a programming specification that works as an interface to allow software components to communicate with each another.

Microsoft allegedly delayed the release of the APIs, knowing they were critical to the development of Novell's office suite applications. The delay meant that Novell could not launch its software packages within 90 days of the release of Windows 95, causing it to lose significant market share to Microsoft's own office suite software, according to Judge Motz's opinion.

The Utah-based software developer had sought more than $1 billion in damages.

Dismissing the suit, Judge Motz said Novell lacked evidence that its applications would have been as successful as those that ran on Windows 95.

"WordPerfect was extremely popular in the 1980s and early 1990s when it ran on many non-Microsoft operating systems," Judge Motz explained in his July 16 ruling. "However, this popularity did not diminish Microsoft's share of the PC operating systems market, which was approximately 90 percent during that period."

As a result, he said, "it cannot reasonably be inferred that if in the years after 1995 Novell's applications ran on operating systems other than Windows, that fact would have challenged Microsoft's monopoly in the PC operating systems market."

The judge added that a "mass exodus" of Novell programmers during this critical time also may have contributed to the delayed release of the software.

"In short, no reasonable jury could find, on the basis of the evidence presented at trial, that Microsoft's withdrawal of support for the … APIs caused Novell's failure to develop its applications within 90 days of the release of Windows 95," he wrote. WJ

Related Court Document:
July 16 opinion: 2012 WL 2913234

Copyright law 'complete preemption' may not doom Texas trade secrets suit

The 5th U.S. Circuit Court of Appeals has reinstated a lawsuit alleging theft of trade secrets and conversion, finding that a Texas federal judge may have jumped the gun on dismissing it under a "complete preemption" analysis.

GlobeRanger Corp. v. Software AG et al., No. 11-10939, 2012 WL 3538494 (5th Cir. Aug. 17, 2012).

The appeals panel reversed and remanded a dismissal order issued by the U.S. District Court for the Northern District of Texas. That court had terminated the case after finding that the plaintiff's allegations were completely preempted by the federal Copyright Act but that it had not pleaded any copyright infringement claims.

GlobeRanger claims that those two companies and the contracting officer passed the technology to Software AG, which then passed it off to the Navy as its own.

GlobeRanger filed suit in a Texas court, alleging misappropriation of trade secrets, conversion, unfair competition, conspiracy and tortious interference. The complaint named Software AG, Software AG USA Inc., Naniq and Main Sail as defendants.

The 5th Circuit found that the case includes plausible allegations that extend beyond the copying of software.

The plaintiff, GlobeRanger Corp., alleges that four rival companies misappropriated its trade secrets in the development and use of a passive radio frequency identification system. The RFID system allows sensors to read electronic tags on products as they are moved around a space, such as warehouse, without having to run each item through a scanner.

The U.S. Department of Defense engaged GlobeRanger to help implement RFID technology throughout its agencies. GlobeRanger in turn employed information technology service companies Naniq Systems LLC and Main Sail LLC as subcontractors to help implement the contracts, according to the appeals court opinion.

As subcontractors, those companies were able to observe how GlobeRanger's RFID worked in the real-world setting of a U.S. Navy warehouse, the opinion said.

The Navy sought to implement a new RFID architecture in 2008. GlobeRanger bid on the contract but lost because, it alleges, a Navy contracting officer and its two subcontractors, Naniq and Main Sail, used their insider positions to steal GlobeRanger's technology.

The defendants removed the case to the Northern District of Texas, saying the federal court had jurisdiction because GlobeRanger's claims were completely preempted by the Copyright Act, 28 U.S.C. § 1338.

Once in federal court, the defendants moved for dismissal on the ground that GlobeRanger had not pleaded any claims upon which relief could be granted.

U.S. District Judge Jane P. Doyle denied GlobeRanger's motion to remand to state court, finding that its trade secrets, conversion and tortious-interference claims are preempted by the federal Copyright Act.

The judge then granted the defendants' motion for dismissal and ordered GlobeRanger to amend its complaint to state a federal copyright claim.

Instead of refiling, GlobeRanger appealed to the 5th Circuit, arguing that its claims were broader than the subject matter of copyright. They included misappropriation of procedures, processes, systems, methods of operation, concepts, principles or discoveries, which are expressly not protected under Section 102(b) of the Copyright Act, the company argued.

The 5th Circuit panel found that the case includes plausible allegations that extend beyond the copying of software.

The court noted that GlobeRanger alleges the defendants "could see how GlobeRanger went about actually deploying onsite, how it set up its readers, how it tagged its product, how it incorporated business process into the design of the warehouse and how it trained sailors."

But, the court said, one of GlobeRanger's claims — the conversion claim — may be federally preempted under the Copyright Act because it alleges the copying of physical property.

The court noted that the complaint asserts that the defendants copied information they obtained from observing GlobeRanger and "hooked it up to the GlobeRanger iMotion server."

The panel reversed and remanded to the District Court, finding that Judge Doyle erred when she dismissed the case so quickly because GlobeRanger plausibly pleaded more than copying of a tangible medium of expression.

"We have only been presented with a question of copyright preemption at the motion-to-dismiss stage. The order of dismissal did not determine whether the complaint plausibly asserted state law claims upon which relief can be granted," the 5th Circuit explained.

"We thus reach only modest conclusions. First, GlobeRanger has pled factual allegations that at least in part fall outside of the scope of copyright. Further, the defendants have argued enough of a basis for preemption on GlobeRanger's conversion claim to stay in federal court," the panel said.

Related Court Document:
Opinion: 2012 WL 3538494

IPHONE GLASS SUIT HAS DEFECTS, JUDGE SAYS

A complaint alleging the iPhone 4's glass panel contains defects failed to meet the heightened pleading standard required when asserting fraud claims, a California federal judge has ruled. The plaintiffs sued Apple Inc. in the U.S. District Court for the Northern District of California, alleging that the company's marketing materials and employee statements led users to believe the iPhone 4's glass panel was indestructible. The class-action complaint included counts for breach of express and implied warranties, unjust enrichment, as well as violations of California's Consumers Legal Remedies Act and false advertising and unfair-competition laws. Apple sought dismissal, arguing that the marketing statements were mere puffery and no reasonable consumer would believe the iPhone's glass was indestructible. The judge granted the motion but allowed the plaintiffs to amend the complaint on all counts except the unjust-enrichment charge.

Williamson et al. v. Apple Inc., No. 5:11-cv-00377, 2012 WL 3835104 (N.D. Cal., San Jose Div. Sept. 4, 2012).

Related Court Document:
Order: 2012 WL 3835104

JUDGE CONSOLIDATES LINKEDIN PRIVACY SUITS

A California federal judge has granted a joint motion to consolidate four actions alleging that LinkedIn Corp. failed to adequately protect user data and negligently allowed hackers to penetrate databases storing sensitive subscriber information. Candyce Paraggua, Katie Szpryka, Scott Shepherd and Sam Veith each sued LinkedIn after hackers breached the website's servers and published on the Internet more than 6 million users' passwords June 6. The four plaintiffs asked the court to consolidate the suits and appoint interim lead class counsel based on the common factual and legal issues presented. The judge granted the unopposed motion and appointed Szypryka's attorney Jay Edelson of Edelson McGuire LLP as class counsel based on his experience with other technology and privacy-related class-action litigation. Kaplan Fox & Kilsheimer's Laurence King will serve as liaison class counsel, the judge said.

Paraggua et al. v. LinkedIn Corp., Nos. 5:12-cv-03088, 5:12-cv-03422 and 5:12-cv-03557, 2012 WL 3763889 (N.D. Cal., San Jose Div. Aug. 29, 2012).

Related Court Document:
Order: 2012 WL 3763889

DROPBOX FACES TRADEMARK INFRINGEMENT SUIT

Dropbox Inc., an online file-hosting service, must defend against an unfair-competition and trademark infringement lawsuit that competitor Officeware Corp. filed in a Texas federal court, despite related proceedings pending before the Trademark Trial and Appeal Board. After Dropbox filed its trademark application for the "Dropbox" mark Sept. 1, 2009, Officeware and two other competitors filed proceedings with the TTAB opposing the mark's registration. Officeware also sued Dropbox in the federal District Court in Dallas, seeking injunctive and declaratory relief. Since 2004, Officeware said, it has used the mark for essentially the same commercial service that Dropbox offers. Dropbox asked to stay the District Court action during the TTAB's opposition proceedings, but the judge denied the motion. The District Court determines infringement independent of the TTAB, and prompt adjudication of this issue outweighs any prejudice to Dropbox, the judge ruled.

Officeware Corp. d/b/a Filesanywhere.com v. Dropbox Inc., No. 3:11-CV-1448, 2012 WL 3262760 (N.D. Tex., Dallas Div. Aug. 10, 2012).

Related Court Document:
Opinion: 2012 WL 3262760

CASE AND DOCUMENT INDEX