Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 5 / AUGUST 14, 2015

WHAT'S INSIDE

COMPUTER FRAUD AND ABUSE ACT

Facebook user's hacking suit against former lover not time-barred

By Patrick H.J. Hughes, Managing Editor, Westlaw Daily Briefing

A Facebook user's suit against her ex-boyfriend for hijacking her account should not have been barred as untimely merely because she had discovered several months earlier that her AOL email account had been hacked, a federal appeals panel has ruled.

Sewell v. Bernardin, No. 14-3143, 2015 WL 4619519 (2d Cir. Aug. 4, 2015).

The statute of limitations on claims stemming from the alleged hacking of the Facebook account ran from the date the account owner discovered it had been compromised, not from the date she first realized her email account had been breached, the 2nd U.S. Circuit Court of Appeals said.

Queens, N.Y., resident Chantay Sewell held several private Internet accounts, including an AOL email account and a Facebook account, the opinion said.

On Aug. 11, 2011, Sewell allegedly discovered she no longer could access her AOL account because the password had been altered. She discovered Feb. 24, 2012, that the same thing had happened to her Facebook account, the opinion said.

On Jan. 2, 2014, she filed a complaint in the U.S. District Court for the Eastern District of New York

REUTERS/Dado Ruvic

against Phil Bernardin, with whom she had a romantic relationship from about 2002 to 2011.

The suit accused Bernardin of impermissibly accessing Sewell's accounts and posing as her in messages that included malicious statements about her sexual activities.

Sewell believed Bernardin was responsible based on Verizon Internet records showing her

CONTINUED ON PAGE 18

COMMENTARY

Efficacy of FCRA claims based on stolen data in data breach cases

Hunton & Williams attorneys John J. Delionado and Jason M. Beach discuss an argument for companies accused of violating the Federal Credit Reporting Act after hackers or other third parties steal data from them.

SEE PAGE 3

41737766

Westlaw Journal Computer & Internet

Published since November 1983

Publisher: Mary Ellen Fox

Executive Editor: Donna M. Higgins

Managing Editor: Donna M. Higgins

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

Managing Desk Editor: Robert W. McSherry

Senior Desk Editor: Jennifer McCreary

Desk Editor: Sydney Pendleton

Graphic Designers: Nancy A. Dubin
Ramona Hunter

Thomson Reuters
175 Strafford Avenue, 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.

For the latest news from Westlaw Journals, visit our blog at http://blog.thomsonreuters.com/westlawjournals.

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: 2015 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."

Westlaw

TABLE OF CONTENTS

Efficacy of FCRA claims based on stolen data in data breach cases

By John J. Delionado, Esq., and Jason M. Beach, Esq.
Hunton & Williams

Plaintiffs often must shoehorn new and evolving factual scenarios into older laws. Data breach litigation is a quickly developing area, and the federal Fair Credit Reporting Act[1] is an older law.

Many people consider the FCRA, enacted in 1970, to be the nation's first privacy law. It was designed to formalize the way the consumer reporting industry had functioned for many years. The FCRA identifies the responsibilities of agencies that create and distribute consumer reports and consumers' rights regarding those reports.

The FCRA contains disclosure obligations for reporting agencies and the users of relevant reports to inform consumers when their reports have been used as a basis for an adverse decision against them. In some cases, these disclosures alert consumers about fraudulent use of their credit accounts or other errors in their credit files that may be the result of faulty reporting or identity theft.[2]

The FCRA's statement of purpose generally calls for "reasonable procedures" designed for the "confidentiality, accuracy, relevancy and proper utilization" of consumer information.[3] To that end, the FCRA details how consumer reporting agencies must assemble and evaluate consumer credit information and other personal details, and how they must provide this information to third parties.

As a strategic matter, the FCRA was an attractive statute for data breach plaintiffs to invoke for subject matter jurisdiction in federal court. A number of data breach causes of action are anchored in state law, including claims for negligence, breach of implied contract, invasion of privacy and unjust enrichment.

As a strategic matter, the FCRA was an attractive statute for data breach plaintiffs to invoke for subject matter jurisdiction in federal court.

For FCRA claims in data breach cases, plaintiffs whose information was stolen or otherwise exposed frequently allege the hacked companies improperly transferred their consumer information to unauthorized third parties. Because the FCRA targets only certain types of entities, some defendants respond that they are not subject to the federal law, arguing they are not "consumer reporting agencies."[4]

Defendants usually challenge standing as well. In fact, the U.S. Supreme Court has decided to review a standing issue under the FCRA in the upcoming term, in *Spokeo Inc. v. Robins*.[5] The Supreme Court's ruling in the case may significantly affect future standing considerations in data-breach-focused FCRA actions, especially where damages or injuries may be difficult to establish.

However, companies that face FCRA claims when data is stolen through a breach or hack have another — simpler — defense: The failure to safeguard stolen data does not qualify as "furnishing consumer reports" under the FCRA.

To illustrate, a case against Countrywide Financial Corp. involved the theft of millions of customers' sensitive personal and financial information. The court found that "[t]he applicable provisions of the FCRA extend liability only where consumer reports are 'furnished' or disseminated in a manner that violates the FCRA."[6]

Noting that the FCRA did not define "furnish," the court held that common sense underscored why Countrywide was not liable under the FCRA: "No coherent understanding of the words 'furnished' or 'transmitted' would implicate Countrywide's action." Instead, a perpetrator independently stole Countrywide's customer information to illegally sell it, the court noted.

Subsequent cases have agreed.

One proposed class action targeted a payment processor after a data breach in 2012. The stolen information included data that could be used to counterfeit new cards. Potentially 1.5 million customers' information was compromised, and the payment

John J. Delionado (L) is a partner with **Hunton & Williams** based in the Miami and Washington offices. His practice focuses on internal investigations, financial institution defense and cybersecurity matters. He can be reached at jdelionado@hunton.com. **Jason M. Beach** (R) is a counsel based in Hunton's Atlanta office whose practice focuses on complex commercial litigation, cybersecurity/data breach issues and government regulatory matters. He can be reached at jbeach@hunton.com. This article presents the views of the authors and does not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.

processor found itself defending, among other causes of action, an FCRA claim.

In dismissing the FCRA claim, the court emphasized that the data was *stolen*, not furnished. The court reasoned that the term "furnish" involves the act of "transmit[ting] information" to another, which is difficult to reconcile with the failure to safeguard stolen data.[7]

The court in *In re Sony Gaming Networks & Customer Data Security Breach Litigation* also dismissed FCRA claims, without allowing the plaintiffs to amend their complaint on this issue, because Sony never "furnished" the stolen data, as required under the FCRA.[8]

Other federal cases similarly demonstrate that the "stolen" distinction can be a critical fact.[9]

The court found it significant that the plaintiff did not allege, and could not plausibly maintain, that Trustwave's "purpose" was to furnish the information to data thieves. Rather, the complaint alleged that Trustwave's purpose was just the opposite: to prevent anyone from getting the information. Although the court allowed the plaintiff to replead the FCRA claim, it warned the plaintiff's attorneys that the FCRA claim, as asserted, raised serious Rule 11 concerns.

CONCLUSION

In sum, "[a]lthough 'furnish' is not defined in the FCRA, courts generally use the term to describe the active transmission of information to a third party rather than a failure to safeguard the data."[12] With Article III standing issues for FCRA claims currently in flux, this simple, commonsense argument can be an effective way to pursue dismissal in data breach cases.

Companies facing FCRA claims when data is stolen through a breach or hack have another — simpler — defense: The failure to safeguard stolen data does not qualify as "furnishing consumer reports" under the FCRA.

Additionally, a dismissal under Federal Rule of Civil Procedure 12 may not be worst outcome for attorneys bringing FCRA claims premised on stolen data.

At least one case has signaled that overreaching FCRA allegations may warrant sanctions under Federal Rule of Civil Procedure 11.[10] The issue arose in a proposed class action arising from a cyberattack on the South Carolina Department of Revenue, which exposed about "3.6 million Social Security numbers, 387,000 credit and debit card numbers and tax records for 657,000 businesses."[11] The defendant was Trustwave Holdings Inc., a Chicago-based data security company that the Department of Revenue had hired to protect its data.

In dismissing the FCRA claim, the court reasoned the allegations did not state Trustwave had some side business to distribute consumer reports. Instead, the plaintiff argued that Trustwave was a consumer reporting agency because it "assembled" consumer data by virtue of the data security services it provided. The plaintiff also contended that Trustwave "furnished" that data as a result of its negligent or willful failure to safeguard the data.

The increase in reported cases addressing FCRA claims after a data breach, along with the threat of Rule 11 sanctions for some of the more creative applications in this context, may signal a decrease in the number of FCRA claims based on stolen data in future breach cases. WJ

NOTES

[1] 15 U.S.C. § 1681.

[2] Lisa J. Sotto, Privacy and Data Security Law Deskbook § 2.01 (2014). The FCRA was amended in 2003 to protect consumers from the growing threat of identity theft.

[3] 15 U.S.C. § 1681(b).

[4] The FCRA places distinct obligations on three types of entities: consumer reporting agencies, users of consumer reports and furnishers of information to consumer reporting agencies. *Chipka v. Bank of Am.*, 355 F. App'x 380, 382 (11th Cir. 2009). Most of the FCRA's requirements, however, generally extend to consumer reporting agencies. "The term 'consumer reporting agency' means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f). Members of the health care, retail and financial services industries who merely pass along information concerning certain debts that are owed to them, or for certain verification purposes, generally are not considered credit reporting agencies. *Falkenberg v. Alere Home Monitoring Inc.*, No. 13-CV-00341, 2015 WL 800378, at *5 (N.D. Cal. Feb. 23, 2015); *Tierney v. Advocate Health & Hosps. Corp.*, No. 13 CV 6237, 2014 WL 5783333, at *3 (N.D. Ill., E. Div. Sept. 4, 2014); *Mirfasihi v. Fleet Mortg. Corp.*, 551 F.3d 682, 686 (7th Cir. 2008); *DiGianni v. Stern's*, 26 F.3d 346, 348 (2d Cir. 1994).

[5] No. 13-1339 (U.S. Apr. 27, 2015). Spokeo.com provides information about an individual, including "contact data, marital status, age, occupation, economic health and wealth level." *Robins v. Spokeo Inc.*, 742 F.3d 409, 410 (9th Cir. 2014), *cert. granted*, 135 S. Ct. 1892 (2015). The plaintiff claimed that Spokeo harmed his employment prospects by reporting he was employed and holding a graduate degree (both of which were untrue) as well as by overstating his wealth. He sued for statutory damages under the FCRA. Although Spokeo asserted that it was not a credit reporting agency, the issue addressed by the 9th Circuit, and now certified by the Supreme Court, is whether violations of statutory rights created by Congress alone are sufficient to satisfy Article III standing. The 9th Circuit reversed the trial court's dismissal order and held that allegations of statutory right violations were sufficient to establish the injury-in-fact prong of Article III standing.

[6] *Holmes v. Countrywide Fin. Corp.*, No. 5:08-CV-00205, 2012 WL 2873892, at *15 (W.D. Ky., Paducah Div. July 12, 2012).

[7] *Willingham v. Global Payments Inc.*, No. 1:12-CV-01157, 2013 WL 440702, at *13 (N.D. Ga., Atlanta Div. Feb. 5, 2013).

[8] 996 F. Supp. 2d 942, 1012 (S.D. Cal. 2014).

[9] *Tierney*, 2014 WL 5783333, at *3 (dismissing FCRA claim when "[p]laintiffs fail to plausibly allege that defendant 'furnished' any information to a third party; rather, plaintiffs allege that computers containing personal information were stolen"). *See also Burton v. MAPCO Exp. Inc.*, 47 F. Supp. 3d 1279, 1287 (N.D. Ala., N.E. Div. 2014) (dismissing FCRA claims in proposed class action when, among other reasons, plaintiffs failed to support that "the theft of credit card information constitutes 'furnishing consumer reports'").

[10] Fed. R. Civ. P. 11(b)(2). Rule 11 requires claims to be "warranted by existing law or by a nonfrivolous argument" that the law should be changed.

[11] *Strautins v. Trustwave Holdings Inc.*, 27 F. Supp. 3d 871 (N.D. Ill., E. Div. 2014).

[12] *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *3 (N.D. Ill., E. Div. Jan. 21, 2015) (dismissing FCRA claims in proposed class action arising from a data breach).

9/11 responders' Facebook records released in disability fraud investigation

By Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals

Retired New York firefighters and police officers are among the 381 Facebook users whose accounts must be released to the Manhattan district attorney's office in its large-scale investigation of fraudulent 9/11-based disability claims, a state appeals court has ruled.

In re 381 Search Warrants Directed to Facebook Inc., No. 14013N, 2015 WL 4429025 (N.Y. App. Div., 1st Dep't July 21, 2015).

Search warrant applications show the district attorney's office reasonably believed the retired civil servants had feigned mental illness to get disability benefits after the Sept. 11, 2001, terrorist attacks and it sought to find evidence on Facebook, the Supreme Court Appellate Division, 1st Department, said.

Facebook asked to quash the 381 warrants, which included nondisclosure provisions, or to be able to alert the targeted users because the searches would essentially reveal every action the individuals had taken on the social networking website, the court's opinion said.

Writing for the three-judge appellate panel, however, Judge Dianne T. Renwick affirmed a trial court's decision dismissing Facebook's motions.

A neutral judge issued the search warrants under the state's criminal procedure laws and Facebook cannot challenge their constitutionality on behalf of the targeted accountholders before criminal charges have been filed, Judge Renwick said.

Responding to the decision, a Facebook representative said the company is considering its options to keep fighting on behalf of people who use its service.

"We continue to believe that overly broad search warrants — granting the government the ability to keep hundreds of people's account information indefinitely — are unconstitutional and raise important concerns about the privacy of people's online information," the representative said.

Joan Vollero, communications director for **Manhattan District Attorney Cyrus R. Vance Jr.**, said the warrants were constitutional, evidence-gathering tools.

"The 1st Department unanimously dismissed Facebook's appeal challenging the validity of judicially ordered search warrants," she said. "In doing so, they became the third court [in this action] to deny Facebook's efforts to block lawful evidence gathering."

Daniel M. Sullivan, an associate at **Holwell Shuster & Goldberg** who filed a friend-of-the-court brief on behalf of Foursquare, Kickstarter, Meetup and Tumblr, explained why the decision raises concerns.

"This is troubling because online platforms have a stake in protecting their users' privacy rights and often raise objections to defective legal process when appropriate," he said.

SOCIAL SECURITY FRAUD?

Two summers ago, the district attorney's office issued the warrants to Facebook based on a large-scale investigation of fraudulent Social Security disability claims, according to the appeals court's decision.

The claims include those from retired police officers and firefighters allegedly feigning mental illness after responding to the 9/11 attack at the World Trade Center, the opinion said.

The warrants said the DA's office had reason to believe these users committed grand larceny, conspiracy and filing of false instruments, according to the opinion.

A 93-page affidavit from a senior investigator at the DA's office supported the application for the warrants, the opinion said.

Facebook asked the office to withdraw the warrants or vacate the nondisclosure provisions, but the government refused, the opinion said.

The DA's office said confidentiality was necessary to prevent the identified individuals from fleeing, destroying evidence or swaying witnesses, according to the opinion.

Facebook asked the New York County Supreme Court to quash the warrants and the nondisclosure provisions, but Justice Melissa C. Jackson denied its requests.

The social networking site appealed, but meanwhile it complied with the warrants, which led to indictments of some of the targeted accountholders, according to the appeals court opinion.

Many times, Facebook evidence contradicted what the defendants told the Social Security Administration, Vollero said.

"To date, 108 people — including four ringleaders — have pleaded guilty to felony charges for their roles in this massive disability fraud scheme," Vollero said.

According to the appeals court opinion, 134 individuals have been indicted based on information obtained in the district attorney's investigation. However, only 62 Facebook users out of the 381 targeted accounts were actually charged with any crime, the opinion said.

Still, the appeals court decided there was no constitutional or statutory authority giving Facebook the right to challenge an allegedly defective warrant before it is executed.

"Neither the Constitution nor New York Criminal Procedure Law provides the targets of the warrant the right to such a pre-enforcement challenge," Judge Renwick wrote, finding no reason to give Facebook a greater right than its users.

PRIVACY PROTECTIONS?

Toward the end of the opinion, Judge Renwick said the appellate panel recognized Facebook's concerns about the scope of the bulk warrants and the district attorney's alleged right to indefinitely retain the seized accounts of the uncharged Facebook users.

The appeals court, however, opted not to rule on these concerns.

"We are disappointed that the court side-stepped an important privacy issue by failing to consider if the district attorney can obtain sweeping warrants for people's Facebook data and indefinitely retain everything in them," said Mariko Hirose, a staff attorney at the New York Civil Liberties Union.

Mariko Hirose, a staff attorney at the **New York Civil Liberties Union** who filed a friend-of-the-court brief supporting Facebook's arguments, commented on this silence, especially when the 2nd Circuit recognized how Fourth Amendment decisions affect the lives of everyday people.

"We are disappointed that the court side-stepped an important privacy issue by failing to consider if the district attorney can obtain sweeping warrants for people's Facebook data and indefinitely retain everything in them," she said.

Albert Gidari Jr., a partner at **Perkins Coie LLP** whose firm filed a friend-of-the-court brief on behalf of technology companies such as Dropbox Inc. and Google, also expressed how the decision is unfortunate for many of the targeted Facebook accountholders.

Most of the 381 identified users "had their entire account histories seized without notice or an opportunity to object, a means to ensure that their data is destroyed or any other remedy at law," he said.

The court defers to the 62 users who were indicted, saying they have an opportunity to challenge the warrants, Gidari noted.

"That doesn't answer for the other two-thirds, nor does it prove that the entire accounts were needed to indict anyone," he said. WJ

(Additional reporting by Peter Hamner, Esq.; editing by Tricia Gorman, Managing Editor, Westlaw Journals)

Attorneys:
Petitioner-appellant (Facebook): Thomas H. Dupree, Gibson, Dunn & Crutcher, Washington

Respondent: Manhattan District Attorney Cyrus R. Vance Jr., New York

Amicus curiae (New York Civil Liberties Union): Jordan Wells, Mariko Hirose and Arthur Eisenberg, New York Civil Liberties Union, New York

Amici curiae (Dropbox etc.): Jeffrey D. Vanacore, Perkins Coie LLP, New York

Amici curiae (Foursquare etc.): Richard J. Holwell, John M. DiMatteo and Daniel M. Sullivan, Holwell, Shuster & Goldberg, New York

Related Court Document:
Opinion: 2015 WL 4429025

See Document Section B (P. 27) for the opinion.

ARBITRATION

TransUnion customer never agreed to terms buried on website, brief argues

By Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals

A federal trial judge in Chicago correctly refused to make a man arbitrate his claims that TransUnion Corp. sells materially misleading credit scores to consumers, according to his appellate court brief.

Sgouros v. TransUnion Corp. et al., No. 15-1371, appellee's brief filed (7th Cir. July 13, 2015).

TransUnion asked the 7th U.S. Circuit Court of Appeals in May to compel Gary W. Sgouros to arbitrate his claims, saying he agreed to arbitration when he clicked an "I accept" button under the website's service agreement (see *Westlaw Journal Computer & Internet*, Vol. 33, Iss. 1, 33 No. 1 WJCOMPI 3).

Sgouros admits he clicked an "I accept" button, but this action only showed he authorized TransUnion Interactive Inc. to obtain his credit information from TransUnion or credit reporting agencies Equifax and Experian.

The plaintiff says a paragraph directly above the button explained this in bold text and never referred to the service agreement, which was set off in an inconspicuous scroll box higher on the website.

Sgouros claims in his brief that he never saw, scrolled through or agreed to TransUnion's service agreement or the arbitration clause buried on page eight of 10 single-spaced pages of dense legalese.

He asks the appeals court to affirm the decision below, denying TransUnion's motion to compel arbitration.

Joseph G. Balice, a civil litigation partner at **Ezra Brutzkus Gubner LLP** in Los Angeles, has been following this case.

He said that with e-commerce becoming the preferred method for buying goods and services, this case is important to see how courts apply old contract doctrines to the new transaction framework.

"In the old days, a consumer was handed what they knew to be a contract and given an opportunity to read and sign it. They may have neglected to read it, but at least they were given the chance," Balice said.

But it may not be the same today.

"Now that commerce has 'evolved,' impetuous consumers are being asked to click through to approve terms and conditions they often ignore because they

might not be sophisticated enough to know what they are entering into by clicking [a button]," Balice said.

CREDIT REPORT PURCHASE

According to court records, Sgouros, a Missouri resident, bought a bundle of products, known as a 3-in-1 Credit Report, Credit Score & Debt Analysis, from TransUnion Interactive on June 10, 2013, for $39.99.

He claims this report was worthless.

According to his complaint filed March 2014, TransUnion never disclosed that it uses a different credit-scoring system than what lenders typically use when evaluating creditworthiness.

The TransUnion credit score Sgorous bought was more than 100 points higher than the credit score reported to a car dealership where he tried to get a loan, the suit says.

Sgouros filed his suit as a potential class action, alleging TransUnion materially misled him and others about the credit scores in the reports it sells.

His suit accuses the Chicago-based company of violating the Fair Credit Reporting Act, 15 U.S.C. § 1681; the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 501/1; and Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010.

CLICKING 'I ACCEPT'

TransUnion filed a motion to compel arbitration, which U.S. District Judge James B. Zagel of the Northern District of Illinois denied. *Sgouros v. TransUnion Corp. et al.*, No. 14-CV-1850, 2015 WL 507584 (N.D. Ill., E. Div. Feb. 5, 2015).

On the webpage, the company's service agreement may have been close to the "I accept" button, but a paragraph of text appeared between them. The paragraph explicitly stated that by clicking the button, users authorized TransUnion to obtain personal credit information from three reporting agencies, Judge Zagel said.

Because there were no explicit instructions for customers to read the embedded service agreement, they reasonably may have assumed they were agreeing to this separate paragraph of text, the judge found.

ARGUMENTS ON APPEAL

In its appellate brief, TransUnion said the visible part of the service agreement, a conspicuous scroll bar in the box and a hyperlink to the printable version, sufficiently gave Sgouros notice about the terms to which he agreed.

Plus, Sgouros clicked a button, showing he accepted the terms, TransUnion argues.

Sgouros disagrees, arguing that TranUnion never notified him or other reasonable consumers to read the terms in the scrollable box and that the "I accept" button only authorized TransUnion to obtain his credit profile from other companies.

He never read the service agreement and never agreed to the arbitration clause, he says, asking the 7th Circuit to uphold Judge Zagel's decision. WJ

Attorneys:
Plaintiff-appellee: Christopher Sanchez, Cafferty Clobes Meriwether & Sprengel, Chicago

Related Court Documents:
Appellee's brief: 2015 WL 4475994
Appellants' brief: 2015 WL 3383278

On the webpage, TransUnion's service agreement may have been close to the "I accept" button, but a paragraph of text appeared between them, the district judge had said.

'I accept': A closer look at agreeing to contracts online

The *Sgouros* case touches upon a very important and troubling issue in the law. Over the last couple of decades, e-commerce has emerged as a preferred method of buying goods and services. In the old days, a consumer was handed what they knew to be a contract and given an opportunity to read and sign it. They may have neglected to read it, but at least they were given the chance.

And the law developed around those kinds of exchanges to determine when and how those contracts and certain key terms — like an arbitration provision, which forces the consumer to waive his constitutional right to a jury trial — are enforceable.

Now that commerce has "evolved," impetuous consumers are being asked to click through to approve terms and conditions they often ignore because they might not be sophisticated enough to know what they are entering into by clicking [an "I accept" button]; and courts are being asked to apply old contract law doctrines to a new transaction framework, and to develop new rules the same way that courts had to develop a rule for contracts entered into over the mail (when ***that*** was a new thing).

–Joseph Balice, partner, Ezra Brutzkus Gubner LLP

Specialty domain seller loses appeal against ICANN over new TLD bidding process

By Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals

The nonprofit managing the Web's domain name system — which allows users to visit websites using words or phrases rather than strings of numbers — has successfully defeated a federal antitrust appeal about its 2012 bidding process for new generic top-level domains.

name.space Inc. v. Internet Corporation for Assigned Names & Numbers, No. 13–55553, 2015 WL 4591897 (9th Cir. July 31, 2015).

Name.space Inc. alleged the Internet Corporation for Assigned Names and Numbers, the global nonprofit known as ICANN, conspired to restrict who could bid on the new generic top-level domains, or gTLDs, but the 9th U.S. Circuit Court of Appeals disagreed.

ICANN has the exclusive authority to manage the domain name system and the "root file zone," which together link numerical Internet Protocol addresses to the corresponding domain, U.S. Circuit Judge Andrew D. Hurwitz wrote for the three-judge panel.

With this authority, ICANN can decide the process of adding new gTLDs, so long as it does not act in a predatory fashion, which name.space never alleged, he said.

The panel affirmed U.S. District Judge Percy Anderson of the Central District of California's decision to dismiss name.space's suit.

John Jeffrey, general counsel of **ICANN**, said the nonprofit was pleased with the dismissal.

"The rules and procedures governing the new gTLD program were created through a global, inclusive, open and multi-stakeholder process, following a bottom-up policy development process leading to consensus-based policy recommendations," he said.

No one at name.space or the company's outside counsel responded to requests for comments.

TOP-LEVEL DOMAINS

Top-level domains are words to the right of the dot in Internet addresses. Before 2000, ICANN offered three main types of TLDs:

- Sponsored TLDs, such as .gov or .edu.
- Country-code TLDs, such as .uk or .fr.
- Generic TLDs, such as .com or .net.

In 2000 and 2012 ICANN expanded the available gTLDs on its root file zone, a master list of all authoritative Web addresses, the 9th Circuit opinion said.

Before this, name.space sold expressive TLDs, such as .sucks and .food, to customers, the opinion said.

These domains, however, were not generally available online. Instead, users needed to change their domain name system settings to visit them through an alternative DNS root, something akin to an alternative Internet, the 9th Circuit said.

ANTITRUST CLAIMS

Name.space sued ICANN in the Los Angeles federal court Oct. 10, 2012, alleging the nonprofit conspired with industry insiders, its board of directors and others to restrain who could bid on gTLDs and monopolized the international market for domain names.

The suit included counts for violations of Sections 1 and 2 of the Sherman Act, 15 U.S.C. §§ 1 & 2; California's analogous Cartwright Act, Cal. Bus. & Prof. Code §16720; and trademark and unfair-competition laws.

Name.space, however, never supported its allegations with proof of a conspiracy; it merely alleged the expensive bidding process favored the dominant, established Internet players, the 9th Circuit opinion said.

> "The rules and procedures governing the new gTLD program were created through a global, inclusive, open and multi-stakeholder process," ICANN's general counsel John Jeffrey said.

BIDDING ON TLDS

When ICANN opened its bidding process for new TLDs in 2012, it published a 349-page guidebook for potential applicants and set an $185,000 application fee for each domain, the opinion said.

Name.space, which had entered the cheaper bidding process in 2000, did not enter the 2012 bidding process, allegedly because of the probative high costs.

The list of applicants in 2012 mainly included industry insiders who bid on 189 TLDs that name.space had been using on its alternative Internet, the opinion said.

Name.space may not have liked how ICANN structured the bidding process, but the company never alleged it was rigged, the appellate court said.

Rather, it was clear ICANN's neutral rules applied to everyone, the court said, dismissing the suit. WJ

Attorneys:
Plaintiff-appellant: Michael B. Miller, Craig B. Whitney and Adam J. Hunt, Morrison & Foerster, New York

Defendant-appellee: Jeffrey A. LeVee, Eric P. Enson and Kathleen P. Wallace, Jones Day, Los Angeles

Related Court Document:
Opinion: 2015 WL 4591897

See Document Section C (P. 34) for the opinion.

Upstate New York sheriff denies unlawfully accessing health records

A New York county, its sheriff and two jail nurses have answered a correction officer's amended federal lawsuit, denying they unlawfully accessed his electronic medical records.

Rodgers v. County of Rensselaer et al., No. 14-cv-01162, answers filed (N.D.N.Y. Aug. 4, 2015).

Responding to a lawsuit corrections officer Kevin Rogers filed in the U.S. District Court for the Northern District of New York, defendants Rensselaer County, Sheriff Jack Mahar, and nurses Katrine Dinan and Elaine Young deny they unlawfully accessed Rogers' medical records, including psychiatric treatment reports, at Samaritan Hospital in Troy, N.Y.

Mahar and Dinan, a county jail nurse, performed discretionary duties as government officials and did not violate any clearly established constitutional or statutory right to privacy Rogers may have had to his medical records, their answer says.

Young, a nursing supervisor at the jail, responded separately to Rogers' suit, saying she acted reasonably in her position and did not cause any of his alleged privacy injuries.

All the defendants have asked the federal court to dismiss Rogers' lawsuit.

UNLAWFUL ACCESS

According to an amended complaint, Rogers has worked as a corrections officer for the Sheriff's Department intermittently since 1990. After Mahar won the sheriff's election in 2003, he began to retaliate against Rogers, allegedly because Rogers supported Mahar's opponent, the suit says.

In April 2004 Mahar fired Rogers based on a false allegation of misconduct, but Rogers successfully challenged the termination and returned to work about two months later, the suit says.

From 2004 until January 2012, Mahar continued to harass Rogers, telling him to go out on disability and assigning him to the least desirable units in the jail without rotating him to better shifts, the suit says. Everyone else was rotated on jail shifts to prevent burnout, Rogers says.

During this time, Mahar also suspended Rogers without pay on five occasions between 2004 and 2011, the suit says.

Rogers says he challenged each suspension, and each time he returned to work with back pay. Cumulatively, he had gone 28 months without a salary, which caused him to file for bankruptcy twice, the suit says.

Since Jan. 30, 2012, Rogers has been on administrative leave without justification or cause and has been refused access to the jail, the suit says.

Rogers says he received notice from Samaritan Hospital in March 2013 alerting him that the jail's staff may have improperly accessed his medical records.

He later found out Dinan accessed and printed out his confidential medical records twice in 2006, and Young accessed them in 2011 without his consent, the complaint says.

County jail nurses are authorized to access inmates' electronic medical records through the hospital's network but are prohibited from unauthorized access, the suit says.

The county has a practice of directing employees to access medical records without proper authorization and failing to supervise, train or discipline them in the proper handling of such records, Rogers alleges.

He seeks compensatory relief from all defendants and punitive damages from Mahar, Dinan and Young. WJ

Attorneys:
Plaintiff: David A. Fallon, Tully Rinckey PLLC, Albany, N.Y.

Defendant (Young): Kevin A. Luibrand, Latham, N.Y.

Defendants (Rensselaer County, Mahar and Dinan): James A. Resila, Carter, Conboy, Case, Blackmore, Maloney & Laird, Albany

Related Court Documents:
Amended complaint: 2015 WL 4692606
Young answer: 2015 WL 4692607
County, Mahar and Dinan answer: 2015 WL 4692605

OpenTV fights Apple bid to dismiss infringement claims for patent invalidity

By Jason Schossler, Contributor, Westlaw Journals

A software maker whose California federal court suit alleges Apple Inc. infringed five patents related to transferring and storing digital content for personalized electronic devices is opposing Apple's argument that two of the patents at issue are invalid and unenforceable.

OpenTV Inc. et al. v. Apple Inc., No. 15-2008, opposition filed (N.D. Cal., San Jose July 17, 2015).

In a June 26 motion to dismiss, Apple said the U.S. District Court for the Northern District of California should toss all allegations based on the two patents because they fail to provide any technological innovations.

OpenTV Inc.'s suit seeks to stop Apple from continuing its allegedly unlicensed use of patented technologies for storing, delivering, playing and viewing interactive content on various mobile devices.

The patents at issue are U.S. Patent Nos. 6,148,081; 6,233,736; 7,055,169; 7,644,429; and 7,725,740.

Apple says the patents describe "well-known abstract" ideas concerning methods or systems for authorizing access to products or information based on certain conditions.

But OpenTV and co-plaintiff Nagravision SA argue the underlying inventions claimed in these patents are "undeniably improvements" to the interactive digital video and TV systems that existed when the patents were filed.

"To accept Apple's effort to recast the claims into alleged abstract ideas, one must strip away the context and plain language of the claims and reduce them to an unrecognizable and irrelevant absurdity," the plaintiffs say in a July 17 opposition brief.

According to the complaint, OpenTV and Nagravision create software for on-demand video services and digital video recorders. The companies' patents belong to a portfolio of more than 4,400 pending and issued patents owned by parent company The Kudelski Group.

REUTERS/Mike Segar

Numerous Apple competitors, including Google, Cisco Systems and Disney, have licensed Kudelski's patent portfolio, according to the complaint.

The suit alleges Apple's iPhone, iPad and other iOS-based mobile devices make "pervasive use" of the plaintiffs' patented technology associated with the downloading and streaming of movie rentals and other digital video information.

By virtue of the plaintiffs' well-known role in the digital media market, Apple knew or should have known that its activities constitute infringement, the suit says (see *Westlaw Journal Computer & Internet*, Vol. 33, Iss. 1, 33 No. 1 WJCOMPI 10).

PATENT VALIDITY

According to Apple, the '081 and '429 patents claim subject matter that is ineligible for patent protection.

The '081 patent concerns the idea of using a "credential" for determining access rights to certain content, and the '429 patent involves a method or system for authorizing "conditional access" to that content, according to the company's June 26 motion to dismiss.

"Both of these ideas have existed for ages and both were used in various fields long before OpenTV filed its patents," the motion says.

The plaintiffs counter this assertion in their opposition, arguing that the court should not permit Apple's "casual dismissal" of the claimed inventions in the patents.

> "Taking Apple's argument to its natural conclusion, the claims are so abstract that they could just as easily cover a medieval castle's drawbridge," the plaintiffs say.

"Taking Apple's argument to its natural conclusion, the claims are so abstract that they could just as easily cover a medieval caste's drawbridge, a padlock with a key, or a 21st-century iris scanner," the plaintiffs say.

The reality is, the claim language specifically "ties the inventions to particular fields and solves particularly technical problems unique to those fields," according to the opposition. WJ

Attorneys:
Plaintiffs: Robert F. McCauley, Finnegan, Henderson, Farabow, Garrett & Dunner, Palo Alto, Calif.

Defendant: George A. Riley and Luann L. Simmons, O'Melveny & Myers, San Francisco

Related Court Documents:
Opposition: 2015 WL 4572967
Motion to dismiss: 2015 WL 4039033
Complaint: 2015 WL 2155461

Apple's DRM tech infringes patents, suit says

By Patrick H.J. Hughes, Managing Editor, Westlaw Daily Briefing

Apple Inc.'s use of the FairPlay digital rights management system to protect its intellectual property rights infringes the IP rights of a Houston-based patent licenser, according to a suit filed in a Texas federal court.

Personalized Media Communications LLC v. Apple Inc., No. 15-cv-1366, complaint filed (E.D. Tex. July 30, 2015).

Personalized Media Communications LLC claims in a suit filed in the U.S. District Court for the Eastern District of Texas that by using FairPlay to distribute encrypted digital content via its various software applications, Apple is infringing its patents.

Personalized Media is the exclusive assignee of U.S. Patent Nos. 8,191,091 and 8,559,635, both of which are called "signal processing apparatus and methods."

This technology is part of Personalized Media's portfolio of more than 80 patents, many of which cover the control of electronic information signals, Personalized Media says.

The company licenses its patented technology to major media companies, such as DirecTV, EchoStar, Motorola and Sony, the complaint says.

FairPlay is a type of DRM technology, the complaint says.

The World Intellectual Property Organization defines DRM as the digital identification and description of IP to enforce a usage restriction. It is used to protect movies, TV shows, e-books, music and apps.

FAIRPLAY

"The FairPlay DRM technology is built into one or more of the iTunes application, App Store application, Apple Music application and the QuickTime multimedia software application," the suit says.

Apple uses the FairPlay technology in its iPhone and iPod devices, as well as its Apple TV, iCloud, iTunes Store, Apple Music and iPad devices, it says.

The receipt and decryption of a FairPlay-protected file by any of these devices practices every step of a claimed method of the '635 patent, it says.

The devices receive FairPlay digital content from the iTunes Store, App Store or another device, Personalized Media alleges. That content is encrypted with a master key that is also encrypted with a random user key corresponding to the user's Apple ID account.

An Apple device can recognize FairPlay-encrypted content and decrypt the information, infringing the '091 patent, the complaint says.

Apple uses the FairPlay technology in its iPhone and iPod devices, as well as its Apple TV, iCloud, iTunes Store, Apple Music and iPad devices, the suit says.

Apple's actions constitute direct patent infringement in violation of Section 271(a) of the Patent Act, 35 U.S.C.A. § 271(a), the complaint says.

According to the complaint, Apple knew of both patents because Personalized Media gave Apple notice and detailed information about Personalized Media's patent portfolio, including information about how the technology covered the FairPlay system.

This knowledge makes Apple a willful infringer and thus liable for treble damages, the complaint says.

Personalized Media also says it had been irreparably harmed from Apple's infringing technology and demands a permanent injunction to halt the continued infringement.

Personalized Media seeks an accounting to determine damages of no less than a reasonable royalty, attorney fees, interest and costs. WJ

Attorneys:
Plaintiff: S. Calvin Capshaw, Elizabeth L. DeRieux and Jeffrey Rambin, Capshaw DeRieux LLP, Gladewater, Texas

Related Court Document:
Complaint: 2015 WL 4593718

REUTERS/Dado Ruvic

Microsoft's Live Preview feature infringes Corel's patents, suit says

By Patrick H.J. Hughes, Managing Editor, Westlaw Daily Briefing

The Live Preview feature found in Word, PowerPoint and other Microsoft programs infringes patents that enable users to preview formatting changes before making them, according to a complaint filed in a Utah federal court.

REUTERS/Mike Blake

Plaintiff Corel Software says Microsoft is liable for both direct and indirect infringement of Corel's patents though the Live Preview feature included in Microsoft Office and other platforms.

Corel Software LLC v. Microsoft Corp., No. 15-cv-528, complaint filed, 2015 WL 4537928 (D. Utah July 27, 2015).

Corel Software LLC, in a suit filed in the U.S. District Court for the District of Utah, accuses Microsoft Corp. of knowingly infringing three patents for Corel's RealTime Preview feature found in WordPerfect, a word-processing program that competes with Word.

Corel Software is the Delaware-based subsidiary of Corel Corp., headquartered in Ottawa, Canada.

According to its website, Corel first gained fame in 1989 when it introduced its graphic design program called CorelDraw.

In 1996 Corel obtained ownership of the WordPerfect program from Novell Inc., a Provo, Utah-based software developer that creates word-processing and desktop-publishing tools.

Three WordPerfect inventors created RealTime Preview to distinguish the program from Microsoft Word by "eliminating computing obstacles between a user's creative vision and the document as it would appear on the page," according to the complaint.

Corel became the exclusive assignee of three patents stemming from the RealTime Preview invention — U.S. Patent Nos. 6,731,309; 7,827,483; and 8,700,996 — each of which is called "Real Time Preview."

The technology allows WordPerfect users to preview the effect of a change to a document before that change is made, the complaint says.

These patents resolve "the slow and inefficient process of selecting among multiple formatting options until the user reaches a desired result," Corel says.

MICROSOFT'S ALLEGED INFRINGEMENT

Corel says the Redmond, Wash.-based computer giant is liable for both direct and indirect infringement of Corel's patents though the Live Preview feature included in Microsoft Office programs.

The infringement is willful because Microsoft knew of Corel's patents when Corel attempted to sell the patents to the company in 2011, the plaintiff claims.

Microsoft likely knew of Corel's RealTime Preview technology as early as 2000, when Microsoft cited the software in the '309 patent in an application it filed with the Patent and Trademark Office, Corel says.

Since 2000 Microsoft has increased the number of uses for its Live Preview feature, an expansion that the plaintiff says was presumably a response to increased consumer demand.

Microsoft has incorporated the Live Preview feature into products beyond Word and PowerPoint, including its OneNote, Visio and Outlook programs, the complaint says.

Microsoft has also induced others to directly infringe the patents by enabling the Live Preview feature by default in its programs, it says.

The "Microsoft Live Preview feature is always present in the infringing products and cannot be used in a substantially noninfringing manner," the plaintiff claims.

According to the complaint, more than 1.2 billion people this year will use Microsoft Office, which includes infringing products that incorporate the Live Preview feature.

Over the next year, more than 100 million PCs will ship with the 2010 version of Microsoft Office preloaded, the complaint says.

Corel seeks treble damages from willful infringement, an accounting, an injunction, attorney fees, costs and expenses. WJ

Related Court Document:
Complaint: 2015 WL 4537928

Smartphone patent is valid, but Samsung did not infringe, jury says

By Patrick H.J. Hughes, Managing Editor, Westlaw Daily Briefing

Samsung Electronics Co. is off the hook for claims it infringed a binary code translation patent for smartphone use, despite an Illinois federal jury's finding that that licensor Cascades Computer Innovation LLC's patent is valid.

Cascades Computer Innovation LLC v. Motorola Mobility Holdings Inc., No. 11-cv-4574, verdict returned (N.D. Ill. July 20, 2015).

The jury, following a trial in the U.S. District Court for the Northern District of Illinois, found that Samsung neither willfully infringed nor induced infringement of the patent.

Samsung attorney **Luke L. Dauchot** of **Kirkland & Ellis** in Chicago said he was pleased with the noninfringement verdict and the "affirmation that a party asserting a patent should not be compensated for technology that is not claimed in the patent."

On July 27 Cascades attorney Raymond P. Niro of Niro, Haller & Niro in Chicago filed an emergency motion for a mistrial on Cascades' behalf, accusing Samsung of submitting improper evidence to the jury.

Niro said the plaintiff "greatly respects the jury process, but its integrity depends on the parties obeying the rules."

SUITS AND SETTLEMENTS

Cascades claims it is the exclusive licensee of U.S. Patent No. 7,065,750, a method patent for preserving exceptions in the binary translation of computer code onto another platform.

In July 2011 Cascades brought suit against Samsung and Motorola Mobility Holdings Inc., claiming they had infringed the '750 patent.

Cascades filed similar suits against various communications companies, including HTC Corp., all of which either use or sell smartphone technologies.

In May 2012 U.S. District Judge Robert Gettleman rejected Samsung and Motorola's motion to dismiss, finding the suit adequately alleged infringement. *Cascades Computer Innovation v. Motorola Mobility Holdings*, No. 11 C 4574, 2012 WL 2086473 (N.D. Ill. May 22, 2012).

Most of the other smartphone makers ended their disputes with Cascades by establishing licensing agreements for the '750 patent.

Samsung and HTC did not settle, however, but rather challenged the validity of the '750 patent, claiming it could not have been infringed.

Samsung and HTC also claimed they were immune from infringement liability because they used Google's Android platform. Cascades had granted Google a license for the '750 patent in January 2014 to resolve their dispute.

All of the defendants, including Samsung and HTC, had their suits consolidated at the claim-construction stage.

In September U.S. District Judge Matthew F. Kennelly said Cascades was barred from seeking damages from Samsung as of the date the Google license went into effect. *Cascades Computer Innovation v. Samsung Elecs. Co.*, 70 F. Supp. 3d 863 (N.D. Ill. 2014).

In January, however, Judge Kennelly allowed Cascade to seek damages for infringing uses that occurred before the license was issued, provided it could prove Samsung infringed the '750 patent. *Cascades Computer Innovation LLC v. Samsung Elecs. Co.*, No. 11 C 4574, 2015 WL 94117 (N.D. Ill. Jan. 6, 2015).

JURY TRIAL

Samsung's validity and infringement claims were tried before a jury beginning July 13.

During closing arguments July 17, Dauchot told the jury that Cascades was "misusing patents to collect money" and that it was holding up its license agreements with the other smartphone makers as "some sort of validation of the '750 technology."

Dauchot said Cascades was acting "as if we were all supposed to pack up our bags and go home because ... eight or so companies" decided when they received Cascades' demand letters that "they would rather pay a relatively small sum of money than put up with the costs of defending a lawsuit."

Niro, in contrast, said Samsung was trying to "trivialize" the reasons other smartphone makers obtained licenses to use the '750 patent, noting that Samsung failed to offer any evidence that the other companies took the license to avoid spending money on litigation.

Because the jury found the patent to be valid, the infringement suit against HTC will proceed. WJ

Attorneys:
Plaintiff: Raymond P. Niro, Arthur A. Gasey, Olivia T. Luk and Christopher W. Niro; Niro, Haller & Niro, Chicago

Defendant (Samsung): Luke L. Dauchot and David Rokach, Kirkland & Ellis, Chicago; Marc H. Cohen, Kirkland & Ellis, Palo Alto, Calif.; Brandon H. Brown, Kirkland & Ellis, San Francisco; Jeanne M. Heffernan, Kirkland & Ellis, New York

Related Court Document:
Jan. 6 order: 2015 WL 94117

Chinese video game maker may sue competitor for source code theft, judge says

By Jason Schossler, Contributor, Westlaw Journals

Shanghai-based video game developer Lilith Games Co. may proceed with claims that a U.S. company stole its software code to create a nearly identical version of its game "Sword and Tower," a federal judge has ruled.

Lilith Games (Shanghai) Co. v. uCool Inc. et al., No. 15-cv-01267, 2015 WL 4128484 (N.D. Cal. July 8, 2015).

The lawsuit, filed in the U.S. District Court for the Northern District of California, alleges uCool Inc. swiped 240,000 lines of Lilith's code and copied it into the source code embodied in the game "Heroes Charge"

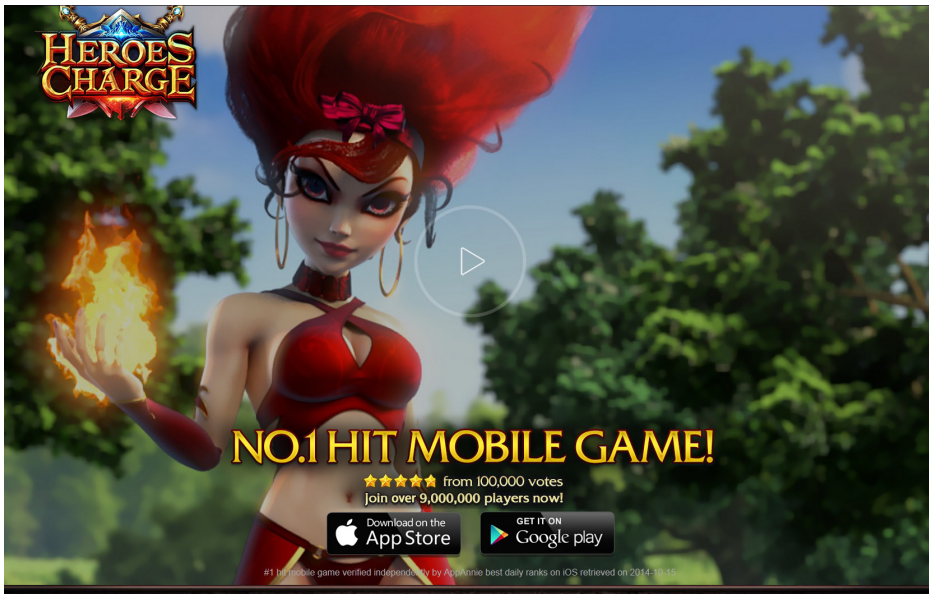
In letting the case move forward, U.S. District Samuel Conti said Lilith adequately pleaded facts showing uCool misappropriated its source code in violation of California's Uniform Trade Secrets Act, Cal. Civ. Code § 3426.

> "Heroes Charge" includes a piece of Lilith Games Co.'s code that triggers Lilith's copyright notice at a certain point during gameplay, the suit says.

Lilith also sufficiently pleaded that uCool knew or had reason to know that the source code was "acquired by improper means or in breach of a duty to maintain its secrecy," according to the judge's order.

However, Lilith's allegations under California's unfair-competition law, Cal. Bus. & Prof. Code § 17200, are preempted by the company's claim for trade secret misappropriation because they essentially restate the same underlying facts, Judge Conti said.

According to the order, Lilith released the game "Dao Ta Chuan Qi," which translates as "Sword and Tower," in China in February 2014, and in the United States and other countries in March 2015.



The lawsuit alleges uCool Inc. swiped 240,000 lines of Lilith Games Co.'s code and copied it into the source code embodied in the game "Heroes Charge," shown here in on a uCool website.

The suit alleges uCool unlawfully obtained access to the copyrighted software code for "Sword and Tower" and used it to create "Heroes Charge," which it published in the United States in August 2014.

Both games involve the same ideas, and the expression of those ideas in both games is virtually identical, the suit says.

"Heroes Charge" includes a piece of Lilith's code that triggers Lilith's copyright notice at a certain point during gameplay, the suit says.

Judge Conti said Lilith pleaded facts providing a "plausible ground to infer" that uCool knew the source code in "Heroes Charge" belongs to Lilith.

"[I]f there was any doubt as to whom the source code belonged, uCool would have known that it was in possession of Lilith's confidential property upon discovering Lilith's copyright notice prominently displayed within 'Heroes Charge,'" he said.

But Judge Conti ruled that Lilith's claims that uCool engaged in unlawful, unfair and fraudulent business practices in violation of the unfair-competition law should be dismissed because they are preempted by the same "operative fact" found in Lilith's Uniform Trade Secrets Act claims.

"Lilith's UCL claims are based exclusively on Lilith's trade secret misappropriation claim," Judge Conti said.

He granted Lilith leave to amend the Uniform Trade Secrets Act claims in the event the company is "able to add allegations to avoid preemption." WJ

Attorneys:
Plaintiff: Teresa J. Michaud and Colin H. Murray, Baker & McKenzie, San Francisco

Defendant: Claude M. Stern and Evette D. Pennypacker, Quinn Emanuel Urquhart & Sullivan, Redwood Shores, Calif.

Related Court Document:
Order: 2015 WL 4128484

TVpad seller settles piracy suit

By Jason Schossler, Contributor, Westlaw Journals

An online retailer that sold TVpad devices preinstalled with a software application that allegedly allowed users to illegally stream Chinese-language programs has settled a copyright infringement lawsuit filed by Dish Network and several program providers.

China Central Television et al. v. Create New Technology (HK) Ltd. et al., No. 2:15-cv-01869, consent judgment entered (C.D. Cal. July 20, 2015).

Defendant NewTVpad Ltd., doing business as Newtvpad.com, and its manager, Liangzhong Zhou, agreed to a consent judgment permanently barring them from distributing the allegedly infringing app or loading it on to any TVpad device, a media-streaming player that transmits programming in several Asian languages.

The judgment in the U.S. District Court for the Central District of California also enjoins the defendants from advertising or promoting unauthorized access to the plaintiffs' copyrighted programming.

An announcement posted on Newtvpad.com states that the company is no longer selling the TVpad or otherwise providing service for the device.

The defendants agreed to settle the suit after U.S. District Judge Margaret M. Morrow granted a preliminary injunction June 11 barring them and several Chinese-based broadcasters from offering free and unauthorized programming on TVpad devices. *China Central Television et al. v. Create New Tech. (HK) Ltd. et al.*, No. 2:15-cv-01869, 2015 WL 3649187 (C.D. Cal. June 11, 2015).

The lawsuit is still pending against lead defendant Create New Technology (HK) Ltd. and nearly a dozen other companies and individuals.

According to the suit, plaintiffs China Central Television, China International Communications Co. and TVB Holdings (USA) Inc. produce the original programming at issue, while Dish holds certain rights to transmit the content in the United States.

The complaint alleged the defendants conspired to set up a pirate broadcasting network that "brazenly captures" CCTV and TVB television channels and video-on-demand programming from Asia and streams the programing over the Internet to U.S. viewers who own a TVpad.

The device is manufactured and sold by some of the defendants and includes access to a free software application store from which users can download a pirating peer-to-peer software app, according to the suit.

In some cases, the devices come pre-installed with the pirating software, the suit said.

The plaintiffs alleged the defendants' activities caused them "irreparable harm" through lost market share and price erosion for programming services (see *Westlaw Journal Computer & Internet*, Vol. 32, Iss. 22, 32 No. 22 WJCOMPI 9).

In granting the preliminary injunction, Judge Morrow said the plaintiffs are likely to succeed on the merits and they would suffer irreparable harm in the absence of preliminary relief.

She also said the plaintiffs are likely to succeed in showing that they own the exclusive rights to transmit the programming in the United States over the Internet in various formats and thus have standing to sue for infringement of those rights.

Other defendants affected by the injunction include China-based Hua Yang International Technology Ltd., California-based Club TVpad Inc. and Florida-based Asha Media Group Inc. doing business as TVpad.com.

The consent judgment signed by Judge Morrow on July 20 states that any violation of the agreement will expose NewTVpad and Zhou to all applicable penalties, including contempt of court.

The plaintiffs seek a permanent injunction, disgorgement of unjust profits, and actual or statutory damages for direct and secondary copyright infringement, trademark infringement, and unfair competition against the remaining defendants. WJ

Related Court Documents:
Order granting preliminary injunction: 2015 WL 3649187
Complaint: 2015 WL 1245560

Software security developer accused of illegally selling products in Iran

A global data security software company violated federal securities laws by failing to disclose to investors that a European subsidiary sold its products to a third-party distributor that possibly resold them in Iran, a recently filed shareholder lawsuit says.

Rossbach v. VASCO Data Security International Inc. et al., No. 15-CV-06605, complaint filed (N.D. Ill. July 28, 2015).

The complaint, filed in the U.S. District Court for the Northern District of Illinois, says VASCO Data Security International Inc. lacked adequate internal controls, resulting in the potential Iran sales and a decrease in the company's stock price.

The suit was filed by VASCO shareholder Linda Rossbach on behalf of all those who purchased the company's stock between Feb. 18, 2014, and July 21, 2015.

A VASCO representative declined to comment on the suit.

The company sells data security software worldwide, specializing in two-factor and digital signature authentication software. It is headquartered in Switzerland and has subsidiaries in Illinois and Belgium.

According to Rossbach's lawsuit, VASCO disclosed in a Form 8-K filed with the Securities and Exchange Commission on July 21 that its European subsidiary sold its products to the third-party distributor.

The distributor might have sold the products to parties in Iran, possibly including parties subject to U.S. economic sanctions, the regulatory filing said.

The company told investors its audit committee initiated an ongoing internal investigation to review the sales with the help of outside counsel. VASCO also said it stopped shipping its products to the distributor pending the results of the investigation, the complaint says.

It further reported working on the sales issue with the U.S. Treasury Department, Office of Foreign Assets Control and the U.S. Department of Commerce, the suit says.

On this news, the software developer's stock price dropped 86 cents, or about 3 percent, the complaint says.

Rossbach claims VASCO did not have a proper mechanism in place to prevent federal laws violations, despite assurances in previous regulatory filings that it had adequate internal controls.

> VASCO Data Security International's misrepresentations about its internal controls and failure to disclose the possible Iran sales caused the stock price to artificially rise, the suit says.

VASCO's misrepresentations about its internal controls and failure to disclose the possible Iran sales caused the stock price to artificially rise, and then drop when the truth emerged, harming its investors, the suit says.

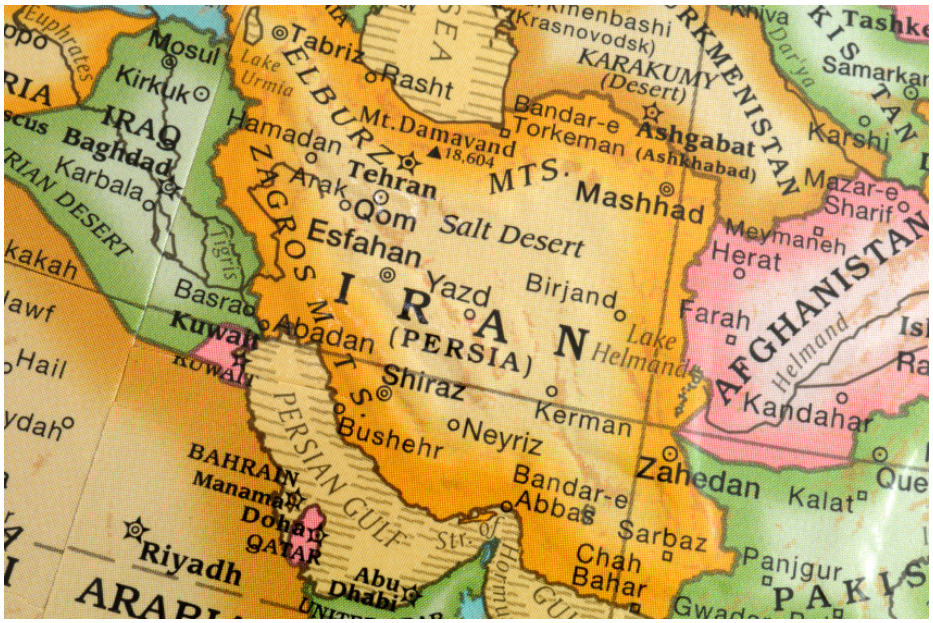
The complaint alleges violations of Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, 15 U.S.C. §§ 78j(b) and 78t(a), and Securities and Exchange Commission Rule 10b-5, 17 C.F.R. § 8 240.10b-5, against VASCO, CEO T. Kendall Hunt and CFO Clifford Brown.

Rossbach is seeking class certification, unspecified damages, and reasonable costs and expenses. WJ

Attorneys:
Plaintiff: Patrick V. Dahlstrom and Louis C. Ludwig, Pomerantz LLP, Chicago; Jeremy A. Lieberman and J. Alexander Hood II, Pomerantz LLP, New York

Related Court Document:
Complaint: 2015 WL 4540355

See Document Section D (P. 40) for the complaint.



Insurer wrongfully denied coverage of $11.5 million cyberattack, suit says

By Thomas Parry, Contributor, Westlaw Daily Briefing

Great American Insurance Co. wrongfully denied coverage for a prepaid debit card company's $11.5 million computer fraud loss claim, according to a Georgia federal court lawsuit.

InComm Holdings Inc. et al. v. Great American Insurance Co., No. 15-cv-2671, complaint filed (N.D. Ga., Atlanta Div. July 28, 2015).

The complaint, filed in the U.S. District Court for the Northern District of Georgia, says Great American acted in bad faith and breached the crime protection policy that it issued to InComm Holdings Inc. by refusing to pay the $10 million policy limit.

Atlanta-based InComm Holdings Inc. and its subsidiary Interactive Communications International Inc. say they promptly informed the insurer that hackers had fraudulently used computers to transfer money between bank accounts.

In addition, Great American's 10-month delay in evaluating the claim and unnecessary information requests exacerbated InComm's damages, the suit says.

'CHIT' SCHEME

In May 2014, InComm became aware that hackers had defrauded the company through duplicate redemptions of prepaid debit cards using its "Vanilla Reload Network" system, the complaint says.

The network system allows customers to add to their debit accounts by purchasing "chits" from vendors and redeeming them online, InComm says.

Hackers allegedly manipulated the computer-based system by sending "multiple, simultaneous redemption requests" that allowed the hackers to use a given chit many times over.

According to the suit, InComm lost nearly $11.5 million as a result of about 25,500 duplicate fraudulent redemptions of more than 2,000 individual reload chits.

In July 2014, InComm submitted its proof of loss claim to Great American under the crime protection policy, which provides coverage for computer fraud, the suit says.

The policy contains a $10 million limit for each occurrence of computer fraud that results in a direct loss through the transfer of money from one "premises" or "banking premises" to a "person or place outside those premises."

InComm says its losses from the scheme should be covered because the fraudulent use of computers directly caused the transfer of money from the plaintiffs' accounts.

COVERAGE DENIAL

After a 10-month investigation and duplicative requests for information, Great American denied the claim, the suit says.

The insurer allegedly contended the losses were not caused by the use of a computer, each fraudulent redemption constituted a separate occurrence and the acts did not cause a transfer of money from the banking premises to an outside party.

In addition, Great American argued the company's losses were due to its contractual liability to fund customer accounts at Bancorp Bank, the suit says.

However, InComm says the thousands of fraudulent redemptions constituted a single occurrence under the policy's language because they were a "series of related acts" sharing the same cause.

"Contrary to Great American's assertions, as a direct result of each fraudulent reload chit redemption comprising the reload chit fraud, InComm was duped into transferring money from InComm's bank account into a separate cardholder account held by one of its issuing bank partners, the Bancorp Bank," it says.

> The insurer's delay and "plainly unreasonable," "frivolous" and "unfounded" refusal to pay constitute bad faith, the suit says.

Great American's delay and "plainly unreasonable," "frivolous" and "unfounded" refusal to pay constitute bad faith, the suit says.

InComm seeks a declaratory judgment that the loss resulting from the chit fraud is covered to the $10 million limit of the policy, a bad faith penalty under Georgia law of 50 percent of the liability limit, interest, attorney fees and costs. WJ

Attorneys:
Plaintiffs: Daniel F. Diffley, Tejas S. Patel and Kristen K. Bromberek, Alston & Bird, Atlanta

Related Court Document:
Complaint: 2015 WL 4559583

Facebook

CONTINUED FROM PAGE 1

accounts were accessed from an IP address associated with a computer at Bernardin's wife's home.

In a separate suit filed May 15, 2013, Sewell accused Bernardin's wife and several Doe defendants of sending phony emails from Sewell's accounts. The action was settled in September 2013.

Sewell maintained in both complaints that she did not provide anyone with passwords to access her accounts.

The suit against Bernardin said his actions violated the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030, which prohibits intentional access to another's computer without authorization.

The complaint also said Bernardin violated Section 2707(f) of the Stored Communications Act, 18 U.S.C.A. § 2707(f), and his actions constituted a trespass to chattels.

On Aug. 2, 2014, U.S. District Judge Arthur D. Spatt dismissed the suit against Bernardin as untimely. *Sewell v. Bernardin*, 50 F. Supp. 3d 204 (E.D.N.Y. 2014).

The suit was time-barred under the CFAA's statute of limitations because it was filed more than two years from the time she discovered her AOL password had been altered, Judge Spatt said.

While Sewell had not discovered until February 2012 that her Facebook account had been hacked, Judge Spatt said she was already aware at that time that "the integrity of her computer had been compromised."

Sewell appealed.

'REASONABLE OPPORTUNITY TO DISCOVER'

Section 1030(g) of the CFAA states that civil enforcement actions must be filed "within two years of the act complained of or the date of the discovery of the damage."

A civil action for violation of the SCA must be brought no "later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation," according to Section 2707(f) of that statute.

The question of the operation of these statutes of limitations was one of first impression in the 2nd Circuit, the panel noted.

It took judicial notice that it is not unusual for an individual to hold numerous Internet accounts with many different user names and passwords, or for a compromise to affect only some accounts.

When Sewell discovered that her AOL account had been impermissibly accessed, she had no reason to believe that her Facebook account had been similarly hacked, the panel reasoned.

While the limitations period for filing CFAA and SCA claims based on access to Sewell's AOL account ended in August 2013, her claims based on access to her Facebook account could be filed as late as Feb. 23, 2014, the panel said.

> When the plaintiff discovered that her AOL account had been impermissibly accessed, she had no reason to believe that her Facebook account had been similarly hacked, the 2nd Circuit panel reasoned.

"She could not reasonably be expected to have discovered a violation that, under the facts as alleged in the complaint, had not yet occurred," the panel said, vacating Judge Spatt's opinion and remanding. WJ

Attorneys:
Plaintiff-appellant: Harvey S. Mars, New York

Defendant-appellee: Gary T. Certain, Certain & Zilberg, New York

Related Court Document:
Opinion: 2015 WL 4619519

See Document Section A (P. 23) for the opinion.

RECENTLY FILED COMPLAINTS FROM WESTLAW COURT WIRE*

Westlaw Citation	2015 WL 4549747
Case Title	Meador et al. v. Apple Inc., No. 6:15-cv-00715 (E.D. Tex., Tyler Div. July 28, 2015).
Case Description	Personal injury, product liability
Factual Allegations	Apple Inc. failed to properly design the iPhone with a lock-out mechanism that is configured to lock out the ability to send or receive texts and other notifications while driving beyond a certain speed threshold, causing a truck driver to collide with plaintiffs' car while using the phone, resulting in the wrongful death of plaintiff's decedent.
Damages Synopsis	Actual and exemplary damages, interest and costs

Westlaw Citation	2015 WL 4554707
Case Title	Sitt v. Local Lighthouse Corp. et al., No. 3:15-cv-05775 (D.N.J. July 24, 2015).
Case Description	Other contract, class action
Factual Allegations	Defendants breached their contracts by falsely representing that they would get the plaintiff's and proposed class members' websites to the first page of search results for Google, Yahoo and Bing for 10 relevant keywords if they made down payments over the phone and agreed to pay defendants for the service.
Damages Synopsis	$30 million as monetary, actual and punitive damages; injunction; fees and costs

Westlaw Citation	2015 WL 4554702
Case Title	Nick v. Target Corp., No. 15-cv-4423 (E.D.N.Y. July 28, 2015).
Case Description	Other fraud, class action
Factual Allegations	Defendant fraudulently scanned the bar code on plaintiff's and other proposed class members' drivers licenses to capture all personal information without consent.
Damages Synopsis	Class certification, statutory damages, injunctive relief, disgorgement, restitution, interest, fees and costs

Westlaw Court Wire is a Thomson Reuters news service that provides notice of new complaints filed in state and federal courts nationwide, sometimes within minutes of filing.

NEWS IN BRIEF

FTC PUBLISHES SECURITY GUIDE FOR BUSINESS

The Federal Trade Commission has published a guide of 10 lessons for businesses to assess their security vulnerabilities and respond to possible risks based on the agency's previous enforcement actions and industry best practices. The guide reminds companies to consider security when managing networks or developing applications. It advises companies to limit the customer data they collect and how long they retain this information. Businesses should also use fictitious data for training or development purposes, restricting access to authorized employees, the guide says. Additionally, the agency recommends requiring complex and unique passwords, which businesses should store as encrypted data, and protections such as two-factor authentication, which adds an extra security layer. For transmitting data, it advises companies to use secure connections, strong cryptography and encryption algorithms. Within the company, networks should be segmented, monitored and tested for vulnerabilities, the guide says. This applies to remote access as well. The guide is available at http://1.usa.gov/1l7SlDo.

CONVICTED HACKING CONSPIRATOR LOSES 4TH CIRCUIT APPEAL

The government sufficiently alleged in a criminal indictment that Brian M. Rich conspired to violate the Computer Fraud and Abuse Act when he accessed LendingTree LLC's network without authorization using compromised credentials, the 4th U.S. Circuit Court of Appeals has ruled. Rich had entered a conditional guilty plea in a Charlotte, N.C., federal trial court, but argued on appeal that the indictment failed to state a claim under the federal hacking law, the appeals court opinion said. The indictment, however, accused Rich and his co-conspirators of unlawfully accessing the online lending exchange's network through an administrator login, the opinion said. Although Rich argued his co-conspirator validly possessed the login information, the indictment also said the credentials were compromised and used without authorization or by exceeding authorized access into the network, the opinion said. The 4th Circuit affirmed the lower court's decision.

United States v. Rich, No. 14-4774, 2015 WL 4547893 (4th Cir. July 29, 2015).

Related Court Document:
Opinion: 2015 WL 4547893

LAW PROFESSORS ASK HIGH COURT TO REVIEW EMAIL SEARCH CASE

A Wisconsin appellate decision allowing police to search and seize more than 16,000 personal emails of someone not under government investigation rebukes centuries-old privacy guarantees for a person's correspondence and papers, four legal scholars have argued to the U.S. Supreme Court. University of California, Irvine School of Law founding dean Erwin Chemerinsky and Instapundit.com founder Glenn Harlan Reynolds are two of the scholars supporting Kelly M. Rindfleisch's *certiorari* petition in her case against the state of Wisconsin. Even before the Constitution's Fourth Amendment was drafted, British colonies in America adopted an English common law decision from 1765 holding the government may not search or seize a person's private papers for evidence of a crime, the friend-of-the-court brief says. These protections are still valid, the brief argues. The high court should review Rindfleisch's case to offer "much-needed guidance" on how search-and-seizure protections apply to electronic communications, the brief says.

Rindfleisch v. Wisconsin, No. 14-1481, amici brief filed (U.S. July 17, 2015).

Related Court Document:
Amici brief: 2015 WL 4481305

CASE AND DOCUMENT INDEX