Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 34, ISSUE 21 / MARCH 24, 2017

WHAT'S INSIDE

PATENT

IBM defeats data security software company's patent appeal

By Melissa J. Sachs

A data security developer's patent designed to stop cybercriminals from stealing information keyed into online forms is invalid, the top patent appeals court has affirmed in a win for IBM.

Trusted Knight Corp. v. IBM Corp. et al., No. 16-1510, 2017 WL 899890 (Fed. Cir. Mar. 7, 2017).

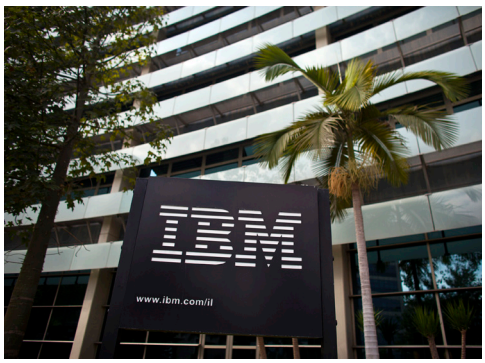
Trusted Knight Corp.'s patent, aimed at blocking key-logging malware that cybercriminals use to scrape users' web form data, was too indefinite to inform others about the invention's scope, the U.S. Court of Appeals for the Federal Circuit ruled.

The U.S. Supreme Court in 2014 interpreted Section 112 of the Patent Act, 35 U.S.C.A. § 112, to require claims to be sufficiently definite to inform those skilled in the art about the scope of what a patent protects. *Nautilus Inc. v. Biosig Instruments Inc.*, 134 S. Ct. 2120 (2014).

The three-judge Federal Circuit panel upheld a lower court's finding that Trusted Knight's patent did not meet this requirement and was therefore invalid.

SLAYING KEYLOGGERS

Trusted Knight is an information technology company based in Annapolis, Maryland, that develops programs to defeat malicious software known as malware.



REUTERS/Nir Elias

In November 2012 the U.S. Patent and Trademark Office issued Trusted Knight U.S. Patent No. 8,316,445, which describes a way of protecting against malware that uses keyloggers, or software that records a user's keystrokes on a computer.

Trusted Knight said its patent improved upon the prior art references, which detect certain keyloggers and then disable or bypass them. The '445 patent does not require the detection of malware.

CONTINUED ON PAGE 6

EXPERT ANALYSIS

Cybersecurity: What are corporate directors' duties?

Holland & Hart attorneys Romaine Marshall and Matt Sorensen discuss the cybersecurity responsibilities for boards of directors and some proactive steps their members can take to protect against shareholder lawsuits.

SEE PAGE 3

41969330

Westlaw Journal Computer & Internet

Published since November 1983

Director: Mary Ellen Fox

Editor:
Melissa J. Sachs
Melissa.Sachs@thomsonreuters.com

Managing Desk Editor:
Robert W. McSherry

Desk Editors:
Jennifer McCreary, Katie Pasek, Sydney Pendleton, Maggie Tacheny

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.legalsolutions.thomsonreuters.com/tag/westlaw-journals.

TABLE OF CONTENTS

Cybersecurity: What are corporate directors' duties?

By Romaine Marshall, Esq., and Matt Sorensen, Esq.
Holland & Hart

Cybersecurity[1] is front page news as organizations large and small suffer losses to data thieves. Nearly all states now require some form of victim notification when sensitive customer or employee information is lost. These notifications are aimed at protecting consumers and can be very expensive for the compromised organization.

While the health care and financial sectors have been regulated for data security and privacy since the 1990s, the Federal Trade Commission has recently received judicial confirmation of its regulatory authority over the security and privacy of consumer data involved in interstate commerce, regardless of industry.

In addition to the direct costs of recovering from a data breach as well as the expense of notifying and providing credit monitoring services to victims, there are potential regulatory fines and lawsuits that can significantly affect an organization's bottom line.

Two types of legal claims are common in the aftermath of data breaches: civil negligence claims that either individuals or a class of victims file against the organization and shareholder derivative lawsuits filed against an organization's board of directors. These latter suits usually claim a breach of a fiduciary duty in failing to prevent the hacking or data security incident.

The lawsuits also typically allege the board failed to monitor compliance with data security requirements, or it demonstrated an intentional disregard for the organization in failing to ensure better data security.

Caremark claims are difficult to prove in practice, requiring a plaintiff to show intentional malfeasance, and courts tend to defer to the decisions of boards.

DIRECTOR DUTY TO MONITOR COMPLIANCE

The legal duties of corporate directors are well established in American jurisprudence. Corporate directors have several fiduciary duties, two of which are the duty of loyalty and the duty of care. Shareholder derivative claims are often colloquially referred to as *Caremark* claims, after a seminal case from Delaware called *In re Caremark International Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

The *Caremark* court held directors owe a duty to monitor that is an extension of the duty of care.

Romaine Marshall (L), a partner at the Salt Lake City office of **Holland & Hart**, helps clients navigate data- and technology-driven business environments and develop solutions to business continuity challenges. He can be reached at rcmarshall@hollandhart.com. **Matt Sorensen** (R) is an associate at the firm. He focuses his practice on domestic and international data privacy and cybersecurity law. He can be reached at cmsorensen@hollandhart.com.

This duty to monitor means directors may not assume the corporation is operating in compliance with the law. They must "assur[e] themselves that information and reporting systems exist in the organization that are reasonably designed to provide to ... the board itself timely, accurate information sufficient to allow ... the board ... to reach informed judgments concerning both the corporation's compliance with law and its business performance."[2]

Caremark claims are difficult to prove in practice, requiring a plaintiff to show intentional malfeasance, and courts tend to defer to the decisions of boards. Under *Caremark*, a plaintiff must show a sustained or systematic failure of the board to exercise oversight or an utter failure to ensure reasonable information and reporting systems exist.

A further refinement to the *Caremark* duty to monitor came in 2006 from the Delaware Supreme Court in *Stone v. Ritter*.[3]

The court reframed the duty to monitor not as an extension of the duty of care, but rather as a function of the duty of loyalty. This distinction is not just semantics.

The duty of loyalty is a category of duties that cannot be eliminated using an "exculpatory clause" or statement placed in the articles of incorporation allowed by Delaware law, which may otherwise limit director liability.

In addition to redefining the duty to monitor as an extension of the duty of loyalty, the *Stone* opinion further raised the threshold to assess a successful claim of breach of the duty to monitor by formulating a new test.

The court held shareholders must demonstrate: an utter failure to implement any reporting or information system or controls or a conscious failure to monitor or oversee such a system if one has been implemented. Both situations require plaintiffs to show the directors knew they were not fulfilling their fiduciary duties.

It is difficult to successfully prove a breach of duty under such a demanding standard.

Despite the high hurdle to prove fault, defending the corporation against a shareholder derivative lawsuit can be a costly exercise, adding additional, unbudgeted expense to a potentially fragile condition resulting from a data breach and the associated recovery process.

In the aftermath of the widely publicized data breaches at Wyndham Hotels in 2008 and 2010, Target in 2013 and Home Depot in 2014, all three corporations have been sued by shareholders asserting *Caremark* or related claims, leading to costly defenses.

WYNDAM HOTELS

Hotelier Wyndam Worldwide Corp. suffered three different cyberattacks between 2008 and 2010, resulting in the loss of hundreds of thousands of consumers' payment card data.

The FTC investigated and filed a lawsuit against Wyndam in 2012. Meanwhile, shareholders demanded that the board investigate the data breaches and hold directors and officers accountable.[4]

- The board discussed the cyberattacks, the company's security policies and proposed security enhancements at 14 meetings between 2008 and 2012.
- The audit committee discussed the same issues at least 16 times during that same period.
- The company hired outside experts to review each data breach and recommend improvements to its security; implementation of the recommendations began after the second breach and continued after the third.
- The board became familiar with the issues.
- The board asked the audit committee to investigate.[6]

Based on these factors, boards of directors and corporate counsel should ensure that similar monitoring efforts are conducted and documented through meeting minutes.

CYBERSECURITY AND CORPORATE GOVERNANCE

Further direction for boards dealing with cybersecurity governance issues can be found from organizations such as the Committee of Sponsoring Organizations of the Treadway Commission, or COSO, and the National Association of Corporate Directors, or NACD.

COSO and COSO Enterprise Risk Management are high-level control frameworks designed or intended to guide the governance of a business enterprise.

> Key risk indicators can help board members ascertain risks and monitor the effectiveness of safeguards, controls and risk-treatment strategies.

When the board declined to bring a lawsuit against the company, disgruntled shareholder Dennis Palkon filed a derivative claim in 2014 against 10 named directors and officers, including CEO and Chairman Stephen Holmes, General Counsel Scott G. McLester and Eric Danziger, CEO of Wyndam Hotel Group LLC. The claims included alleged breach of fiduciary duty and unjust enrichment.[5]

The shareholder derivative lawsuit against Wyndham's directors and officers was eventually dismissed. Key factors in the court's dismissal included:

Recognizing a need for a more complete and relevant corporate governance framework that addresses information security and privacy governance, in 2005 the National Cyber Security Summit's corporate governance task force recommended for COSO to revise its internal control/integrated framework to explicitly address information security governance.[7]

In January 2015, COSO published "COSO in the Cyber Age," a long overdue publication that provides guidance on cybersecurity controls in the context of corporate governance.[8]

Further support for considering information security an essential part of corporate governance can be found in the Business Roundtable's 2005 publication, "The Principles of Corporate Governance."[9]

Currently, the NACD offers corporate directors a cybersecurity resource center and works through Carnegie Mellon University to offer corporate directors a certificate in "cybersecurity oversight."

SOME DIRECTOR RESPONSIBILITIES AND OVERSIGHT TASKS

The *Wyndam* case was ultimately dismissed under a Delaware doctrine known as the business-judgment rule.

This rule gives directors wide latitude to make business decisions and take risks, even when the outcomes result in severe company losses.

In essence, the Delaware courts do not want to second-guess directors' business decisions. To the courts, it is also not a breach of a fiduciary duty to make what turns out to be an unprofitable business decision.

Courts consider a variety of relevant facts and actions to demonstrate boards of directors have upheld their duty to monitor compliance with regard to cybersecurity.

These include common sense measures boards can consider and implement to meet their fiduciary duties. The following actions might be appropriate for a board of directors to consider to improve oversight of the organization's information security program:

- Adopt principles from "COSO in the Cyber Age" into the organization's existing governance model.
- Review and approve the organization's information security policy. These are not information security standards, procedures or specifications dealing with technology configuration. Rather, an enterprise information security policy should delegate information security management responsibility and accountability to executives and business units. The policy may also state the selected regulatory framework, regulated data designations and classifications, and intent to maintain the security program. The policy might also contain statements directed to the enterprise workforce regarding minimum acceptable behaviors and

requirements on such topics as: employee awareness, annual security training, use of corporate information and information technology resources, and any duty to report observed violations and suspicious activities.

- Review and address summary reports based on risk and compliance assessments and audits. Key findings and proposed remediation plans can be distilled into a high-level strategic roadmap and risk-treatment plan that the board may review periodically.
- Based on the approved roadmap and risk-treatment plan, approve the allocation of resources and funds to the information security and data privacy programs. Funding should be allocated for hiring and training people to address gaps in the information security program. The risk-treatment plan may include proposals for risk-transfer mechanisms including insurance for data loss, business interruption and damages stemming from computer intrusion events.
- The board should serve as check and a balance against over-aggressive business uses of regulated data, particularly when business plans rely on the collection, sharing, and use of sensitive personally identifiable information belonging to consumers, customers, business partners and foreign citizens. Board members should expect an accounting from executives regarding compliance to personal data protection laws as well as the corporation's honoring of commitments made to consumer via privacy policies and participation in international personal data transfer commitments.
- The board may choose to form or leverage an existing enterprise risk committee to integrate information security risk into the overall enterprise risk-management program and to help prepare and communicate key messages to the entire board.
- Boards of directors can hire outside experts to provide director specific cybersecurity literacy training. Organizations such as the NACD provide many resources to support boards in executing the responsibility to strengthen information security oversight.
- The board should not assign accountability over information security to one single executive such as a chief information officer. Burying information security accountability under a single executive risks shielding the board from important weaknesses that often lead to the very compromises reported in widely publicized hacking incidents and data breaches. Information security is a multidisciplinary endeavor that includes technology, across-enterprise business processes, legal, and compliance concerns. Reporting structures for information security often move information security officers out from under technology-heavy roles like chief information or technology officers, and may include multiple direct and dotted-line accountabilities to the CEO, general counsel, compliance or chief operations officers.

Information security is a multidisciplinary endeavor that includes technology, across-enterprise business processes, legal and compliance concerns.

If they are not already part of regular board discussions and reports, a number of these steps and activities are recommended.

EXAMPLE KEY RISK AND PERFORMANCE INDICATORS

Key risk indicators can help board members ascertain risks and monitor the effectiveness of safeguards, controls and risk-treatment strategies.

Key indicators of potential risk to information technology and sensitive data include:

- Pending merger and acquisition plans: boards must ensure due diligence includes some degree of cybersecurity due diligence.
- Frequency and severity of security incidents, including those that do not affect sensitive data. Examples include website defacements, denial-of-service attacks, nonsensitive data exposures and losses, as well as insider attacks.
- Amount of turnover and number of unfilled positions in the information security function.
- Employee ratio of information security professionals to information technology professionals, knowing ideal ratios will differ across organizations and industries.
- Percentage of overall IT budget dedicated to security.
- Diversity and complexity of operations, including geographical, geopolitical and impact of social issues giving rise to hacktivism.
- Industry-specific threat analyses.
- Audit and compliance report findings, including significant or high-risk findings recurring over multiple years.
- Education and training investments resulting in the number and type of professional certifications held by specialist-employees.
- Cooperation and integration of compliance, legal, risk and IT functions.

ACTION PLAN AND ROADMAP

The following outline suggests an action plan for assessing and improving your board's ability to oversee and monitor the enterprise information security program, which is a key component to fulfill its fiduciary duty obligations.

- In the very near term, review the prior 12 to 18 months of board meeting minutes. Look for references to or indicators of information security governance activities. If lacking, ensure board meetings include such topics and that deliberations and decisions are documented in board minutes.
- Within 30 days, discuss the topic of board awareness with the CEO, general counsel, chairman or audit or risk committee chair. Propose an enterprise cybersecurity risk assessment. Work to improve alignment of executive leadership on the topic.
- Within the next three to six months, source and initiate an enterprise risk assessment, augmenting internal

capabilities with outside expertise as needed. Once the assessment is completed, review the results with key stakeholders and propose a risk-treatment plan for major enterprise cybersecurity risks. Included in the plan will be key decisions or recommendations to accept, mitigate or transfer certain risks. Present the plan to the board and seek necessary accountabilities, assignment of cross-functional authorities, and funding to coordinate and implement the plan.

- Between six and 12 months, work to implement the controls outlined in the plan to mitigate key risks, secure suitable insurance coverage and monitor the program through regular testing of established controls. Include an annual cybersecurity incident response plan test, simulating a large data breach.

CONCLUSION

Data breaches may be inevitable to some degree, but the severity and frequency can be addressed with time-tested governance approaches.

Boards that can proactively guide their organizations to the inevitable realization of the true cost of doing business in modern threat-filled, interconnected commercial cyberspaces will have the advantage over those who learn the hard way through litigation and regulatory penalties.

Boards of directors best serve shareholder interests when they adapt existing corporate governance structures to include oversight of cybersecurity and data privacy. WJ

NOTES

[1] The term cybersecurity is often used interchangeably with information security or data security. While these terms all have different definitions accepted by professionals they often are used interchangeably. Cybersecurity commonly denotes internet-related risks and security while information security refers to a broader domain that includes information risk beyond that posed by internet-based threats.

[2] *In re Caremark Int'l Derivative Litig.*, 698 A.2d 959, 970 (Del.Ch. 1996).

[3] *Stone v. Ritter,* 911 A.2d 362 (Del. 2006).

[4] Timothy Cornell, *Wyndham – A Case Study in Cybersecurity: How the Cost of a Relatively Small Breach Can Rival That of a Major Hack Attack,* Metropolitan Corp. Counsel (Mar. 19, 2015, 9:50 AM), http://bit.ly/1BbpvNY.

[5] Vin Gurrieri, *Wyndham Execs Slapped With Investor Suit Over Data Breach,* Law360 (May 6, 2014, 3:02 PM), http://bit.ly/2mjUoQc.

[6] *Palkon et al. v. Holmes et al.,* No. 14-cv-1234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

[7] *See* National Cyber Security Summit Task Force, *Information Security Governance: A Call to Action* (Apr. 2004), http://bit.ly/2mECISZ.

[8] Mary E. Galligan, Kelly Rau & Deloitte & Touche LLP, *COSO in the Cyber Age* (Jan. 15, 2015), http://bit.ly/2mDqdrX.

[9] *2010 Principles of Corporate Governance,* Business Roundtable (Apr. 1, 2010), http://bit.ly/2mEB4AV. As part of its oversight function, the board should designate senior management who will be responsible for business resiliency. The board should periodically review management's plans to address this issue. Business resiliency can include such items as business risk assessment and management, business continuity, physical and cybersecurity, and emergency communications.

IBM

CONTINUED FROM PAGE 1

Almost two years later, in August 2014, the data security firm sued IBM and its cybersecurity division Trusteer Inc. in Delaware federal court for infringement of the '445 patent.

In September 2015 the court held a claim construction hearing, during which each side offered its interpretations of the patent's language.

IBM and Trusteer told the court some terms were indefinite under Section 112 of the Patent Act, referring to the language that described how the patent "responds to software key logging" and how it "passes encrypted data to an access level where certain keyloggers operate."

U.S. District Judge Leonard P. Stark of the District of Delaware agreed with IBM and Trusteer that these two terms failed the high court's indefiniteness test. *Trusted Knight Corp. v. IBM Corp.*, No. 14-cv-1063, 2015 WL 7307134 (D. Del. Nov. 19, 2015).

A person with ordinary skill in the art would not know the meaning of them with reasonable certainty, the judge said.

DISPUTED PHRASES

Regarding the first disputed phrase, Judge Stark pointed out how Trusted Knight said the invention does not respond to or detect malware. With that premise, he said it was unclear what exactly happens in response to software key-logging.

> The panel concluded Trusted Knight failed to inform those with ordinary skills in the art about the scope of the '445 patent.

As for the second disputed phrase, the parties agreed there was a typographical error in the patent. Judge Stark said the error could not be easily corrected because Trusted Knight's proposed language was subject to reasonable debate, which would affect the patent's scope.

Based on Judge Stark's indefiniteness rulings on these terms, the parties stipulated to a final judgment on invalidity, and Trusted Knight appealed to the Federal Circuit.

The three-judge panel affirmed Judge Stark's findings.

The panel concluded the disputed phrases in Trusted Knight's patents were ambiguous and failed to inform those with ordinary skills in the art the scope of the '445 patent. WJ

Attorneys:
Appellant: Paul R. Gupta, Reed Smith LLP, San Francisco, CA; Gerard M. Donovan, Reed Smith LLP, Washington, DC; Rudolph E. Hutz, Reed Smith LLP, Wilmington, DE; James C. Martin, Reed Smith LLP, Pittsburgh, PA

Appellees: David A. Nelson, Quinn Emanuel Urquhart & Sullivan, Chicago, IL; John T. Mckee and Alexander Rudis, Quinn Emanuel Urquhart & Sullivan, New York, NY

Related Filings:
Opinion: 2017 WL 899890
Reply brief: 2016 WL 3586827
Defendants' brief: 2016 WL 3251100
Opening brief: 2016 WL 1546780
First amended complaint: 2015 WL 5049809

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

Smartflash's patents nixed on appeal in spat with Apple

By Patrick H.J. Hughes

Apple Inc. has convinced the top patent appeals court to invalidate three of Smartflash's data storage patents following a dispute in which a jury slapped the iPhone maker with a $533 million infringement bill.

Smartflash LLC et al. v. Apple Inc., No. 16-159, 2017 WL 786431 (Fed. Cir. Mar. 1, 2017).

While the $533 million award was awaiting reconsideration, the U.S. Court of Appeals for the Federal Circuit said Apple's motion for a directed verdict over the patents' validity should have been granted.

The three-judge Federal Circuit panel said Smartflash's inventions failed the test established by the U.S. Supreme Court in *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S. Ct. 2347 (2014), for finding whether software patents are abstract.

BLOCKING 'DATA PIRATES'

Smartflash is a data storage technology company based in the British Virgin Islands with a unit in Tyler, Texas.

Among its many patents currently in litigation with Apple, Google and other tech giants, Smartflash is the exclusive assignee of U.S. Patent Nos. 7,334,720; 8,118,221; and 8,336,772, all of which are titled "data storage and access systems."

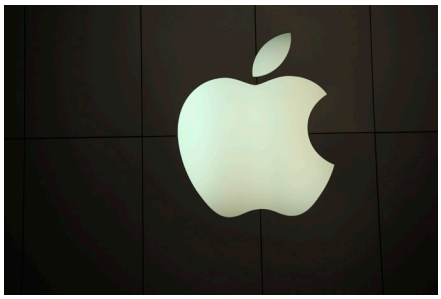
In addition to having identical titles, the '720, '221 and '772 patents included much of the same language and a specification that said they were meant to counter "the growing prevalence of so-called data pirates."

The panel noted that these pirates were gaining access to data by either legitimate or unauthorized means and then made this content available on the internet without authorization.

The inventors of the patents sought to address the problem with a system of data "carriers" that could receive and validate payments from users in exchange for data.

SMARTFLASH LITIGATION

Smartflash sued Apple in 2013 in the U.S. District Court for the Eastern District of Texas for infringement of numerous patents.



REUTERS/Robert Galbraith

Among its defenses, Apple filed a motion for summary judgment seeking to invalidate the '720, '221 and '772 patents as abstract pursuant to Section 101 of the Patent Act, 35 U.S.C.A. § 101.

U.S. District Judge Rodney Gilstrap denied the motion. *Smartflash LLC v. Apple Inc.*, Nos. 13-cv-447 and 13-cv-448, 2015 WL 661174 (E.D. Tex. Feb. 13, 2015).

The judge said the patents passed the two-step *Alice* inquiry, which first asks whether an invention is "a law of nature, a natural phenomenon or an abstract idea."

While Judge Gilstrap found the '720, '221 and '772 patents recited abstract ideas and therefore did not pass the first stage of the inquiry, he said the patents transformed those ideas into patent-eligible inventions, passing *Alice*'s second step.

A jury later found Apple liable for $533 million for infringing the three patents. *Smartflash LLC v. Apple Inc.*, No. 13-cv-447, 2015 WL 1228116 (E.D. Tex. Feb. 24, 2015).

In July 2015 Judge Gilstrap vacated the $533 million award after Apple complained that the damages had been improperly calculated.

However, the judge said the validity and infringement decisions should stand. *Smartflash LLC v. Apple Inc.*, No. 13-cv-447, 2015 WL 11089752 (E.D. Tex. Sept. 2, 2015).

Apple appealed.

'INVENTIVE CONCEPT'?

The Federal Circuit agreed with Judge Gilstrap that the patents were directed to an abstract idea, and then weighed whether the inventions included an "inventive concept" that would make them patent eligible.

The panel noted the Supreme Court in *Alice* held that routine computer activities are insufficient for conferring patent eligibility.

Smartflash, however, argued that these patents were not routine, and were "akin" to a patent the Federal Circuit found eligible in *DDR Holdings LLC v. Hotels.com LP*, 773 F.3d 1245 (Fed. Cir. 2014).

The Federal Circuit said Smartflash's patents were not similar to the one in *DDR Holdings*.

Rather, the panel called the three Smartflash patents "analogous" to an online system for advertising that the appeals court said was not patent-eligible in *Ultramercial Inc. v. Hulu LLC*, 772 F.3d 709 (Fed. Cir. 2014).

Smartflash's technology covered reading, receiving and responding to payment validation data, the panel said.

"This is precisely the type of internet activity that we found ineligible in *Ultramercial*," the panel said, concluding Smartflash's patents failed to recite any inventive concept. WJ

Attorneys:
Plaintiffs-appellees: Aaron M. Panner, Kellogg, Huber, Hansen, Todd, Evans & Figel, Washington, DC; Nicholas O. Hunter, John A. Curry, Jason D. Cassady, Bradley W. Caldwell, John F. Summers and Hamad M. Hamad, Caldwell Cassady & Curry, Dallas, TX

Defendant-appellant: Mark A. Perry, Gibson, Dunn & Crutcher, Washington, DC; Brian Buroker and Hervey M. Lyon, Palo Alto, CA

Related Filings:
Opinion: 2017 WL 786431
Motion for summary judgment: 2014 WL 7794903
Complaint: 2013 WL 2338055

Capital One, insurers prevail in pair of patent appeals

By Patrick H.J. Hughes

The Federal Circuit has let stand lower court rulings letting Capital One Financial Corp. and several insurance companies off the hook for allegedly infringing Intellectual Ventures' patents.

Intellectual Ventures I et al. v. Capital One Financial Corp., No. 16-1077, 2017 WL 900031 (Fed. Cir. Mar. 7, 2017).

Intellectual Ventures I et al. v. Erie Indemnity Co. et al., Nos. 16-1128 and 16-1132, 2017 WL 900018 (Fed. Cir. Mar. 7, 2017).

In a pair of decisions, a panel of the U.S. Court of Appeals for the Federal Circuit ruled that the patents Intellectual Ventures asserted against Capital One and the insurers were invalid as abstract.

Bellevue, Washington-based Intellectual Ventures owns a portfolio of roughly 3,500 patents. It is considered one of the world's largest patent holders, often labeled a patent assertion entity due to the patents it asserts against a variety of corporations.

The Federal Circuit panel ruled that three patents that Intellectual Ventures had asserted against Capital One and another two it claimed Erie Insurance Co. and Old Republic General Insurance infringed were invalid under Section 101 of the Patent Act, 35 U.S.C.A. § 101.

The lower courts did not err in finding the technologies unpatentable under the standard the U.S. Supreme Court set in *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S. Ct. 2347 (2014).

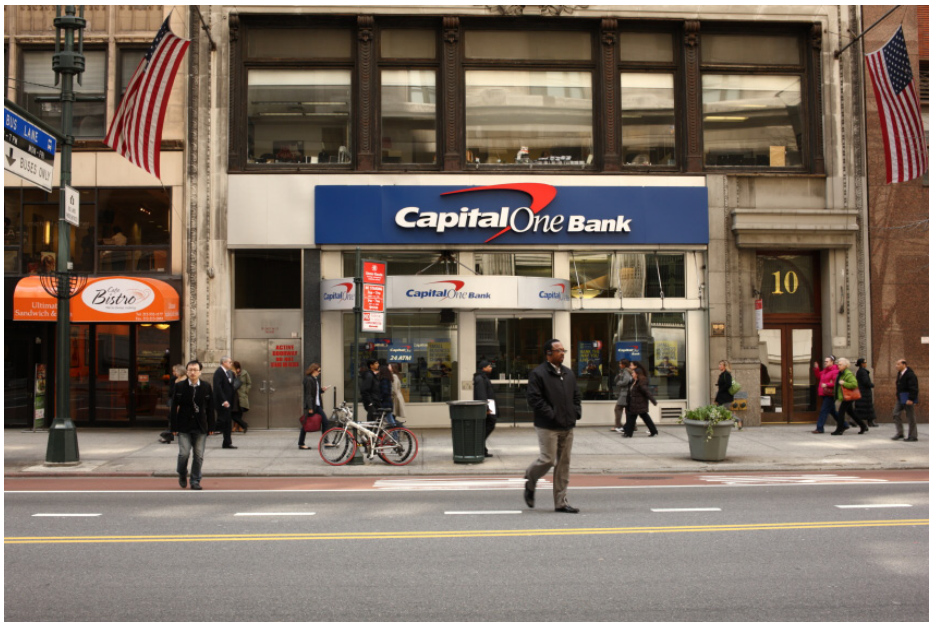
Courts use the *Alice* standard for evaluating whether an invention is "an abstract idea" and, if so, whether it transforms that idea into "an inventive concept," the panel said.

CAPITAL ONE

Among its slew of patents, Intellectual Ventures owns U.S. Patent Nos. 6,546,002; 7,984,081; and 6,715,084, which cover technologies involved in the retrieval and organization of data.

Intellectual Ventures sued Capital One and several subsidiaries in the U.S. District Court for the District of Maryland in January 2014, claiming infringement of all three patents.

The Capital One companies admitted using systems that infringed the patents but moved for summary judgment on the ground that the patents were invalid.



The defendants also made antitrust counterclaims, saying Intellectual Ventures was abusing its monopoly power in violation of Section 2 of the Sherman Act, 15 U.S.C.A. § 2, and Section 7 of the Clayton Act, 15 U.S.C.A. § 18.

Those claims survived Intellectual Ventures' motion to dismiss and are pending under seal. *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, No. 14-cv-111, 2015 WL 4064742 (D. Md. July 1, 2015).

Meanwhile, in a different infringement proceeding, U.S. District Judge Alvin K. Hellerstein of the Southern District of New York ruled that the '084 patent was invalid. *Intellectual Ventures II LLC v. JPMorgan Chase*, No. 13-cv-377, 2015 WL 1941331 (S.D.N.Y. Apr. 28, 2015).

A few months later, in the case against Capital One, U.S. District Judge Paul W. Grimm in Maryland found the '081 and '002 patents invalid. *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 127 F. Supp. 3d 506 (D. Md. 2015).

Judge Grimm also said that under the doctrine of collateral estoppel, Judge Hellerstein's decision barred Intellectual Ventures from claiming the '084 patent had been infringed.

On appeal, the Federal Circuit affirmed all the invalidity rulings and the collateral estoppel decision.

Applying the *Alice* analysis, Chief U.S. Circuit Judge Sharon Prost, writing for the panel, said the '081 patent does not transform an abstract idea into a patentable subject matter.

"We perceive no 'inventive concept' that transforms the abstract idea of collecting, displaying and manipulating XML data into a patent-eligible application of that abstract idea," the judge wrote on behalf of Circuit Judge Evan Wallach and Circuit Judge Raymond Chen.

The panel also rejected Intellectual Ventures' argument that Judge Grimm erred in certifying the case for interlocutory appeal given that Capital One's antitrust counterclaims remained pending.

Noting that Intellectual Ventures' patent infringement suit involves only "a narrow subset" of the patents involved in the antitrust dispute, Judge Prost said "the scope of Capital One's antitrust counterclaims transcends issues of mere infringement."

The panel left its analysis of the '002 patent's validity to the "companion appeal" filed by insurers Erie and Old Republic.

ERIE AND OLD REPUBLIC

Intellectual Ventures filed a series of suits in the U.S. District Court for the Western District of Pennsylvania on Aug. 22, 2014, claiming that Erie and Old Republic had infringed the '002 patent and two of its other patents, U.S. Patent Nos. 6,519,581 and 6,510,434, which relate to collecting information and retrieving information across a communications link.

U.S. District Judge Mark R. Hornak ruled Sept. 25, 2015, that all three patents were invalid as abstract and dismissed the suits. *Intellectual Ventures I LLC v. Erie Indem. Co.*, 134 F. Supp. 3d 877 (W.D. Pa. 2015).

Judge Hornak described the '581 patent as "extraordinarily broadly drawn" and the '434 patent as including a concept that was "simply not inventive."

He said the '002 patent did not include claims that pointed to an inventive concept. Rather, "they point in the opposite direction," he said.

On appeal, the Federal Circuit found no error in any of the invalidity findings, echoing Judge Hornak's assessment of the '581 and '434 patents.

As to the '002 patent, Judge Prost said it "identifies a need, but the claims fail to provide a concrete solution to address that need." WJ

Attorneys:
Plaintiffs-appellants: Ian N. Feinberg, Feinberg Day Alberti & Thompson, Menlo Park, CA; Christian J. Hurt, Nix Patterson & Roach, Dallas, TX

Defendants-appellees: Matthew J. Moore, Latham & Watkins, Washington, DC; Gregory H. Lantier, Wilmer Cutler Pickering Hale & Dorr, Washington, DC; Vernon M. Winters, Sidley Austin LLP, San Francisco, CA

Related Filings:
Opinion (Capital One): 2017 WL 900031
Opinion (Erie): 2017 WL 900018
Complaint (Old Republic): 2014 WL 4684036
Complaint (Erie): 2014 WL 4684039
Complaint (Capital One): 2014 WL 2822400

See Document Section B (P. 23) for the Capital One opinion and Document Section C (P. 30) for the Erie opinion.

PATENT

Nintendo prevails in inventor's patent case over 3-D game console

(Reuters) – A federal appeals court handed Nintendo Co. a victory March 17 in a long-running lawsuit in which the game console maker had been accused of copying patented 3-D imaging technology.

Tomita Technologies USA et al. v. Nintendo Co. et al., No. 16-2015, 2017 WL 1034471 (Fed. Cir. Mar. 17, 2017).

The U.S. Court of Appeals for the Federal Circuit affirmed a lower court judge's determination that Nintendo's 3DS gaming console does not infringe on a patent owned by Tomita Technologies International Ltd., a company controlled by Japanese inventor Seijiro Tomita.

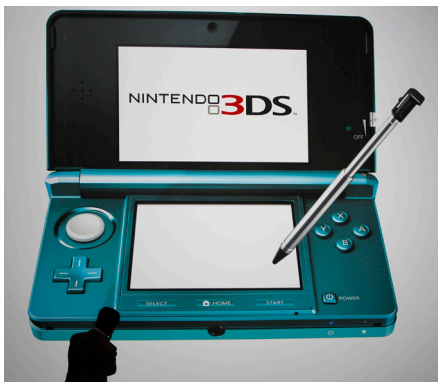
In a decision by Circuit Judge Evan Wallach on behalf of a unanimous panel that also included Judges Sharon Prost and William Bryson, the Federal Circuit held that U.S. District Judge Jed Rakoff in Manhattan did not err in finding Nintendo's approach to creating 3-D images was different than the method described in Tomita's patent.

Tomita's patent describes a method of producing 3-D visuals without the use of 3-D glasses. Tomita sued Nintendo for infringement in 2011 in the U.S. District Court in Manhattan. The inventor alleged that he showed a prototype of his technology to Nintendo officials during a 2003 meeting.

During a 2013 jury trial, Tomita's lawyers sought about $290 million in damages, arguing he was entitled to $9.80 for every 3DS console Nintendo sold until that point in time.

The jury found that Nintendo infringed but awarded Tomita just $30 million. Judge Rakoff later halved the verdict to $15 million, finding that jurors used an improper approach to calculating damages. *Tomita Techs. v. Nintendo Co.*, No. 11-cv-4256, 2013 WL 4101251 (S.D.N.Y. Aug. 14, 2013).

Nintendo appealed to the Federal Circuit, which held Judge Rakoff had improperly construed a key claim in the patent. The court vacated the verdict and instructed Judge Rakoff to decide whether Nintendo's patent infringes under its revised claim construction. *Tomita Techs. v. Nintendo Co.*, 594 Fed. Appx. 657 (Fed. Cir. 2014).



REUTERS/Toru Hanai

The patent at issue covers a method of producing 3-D visuals. The plaintiff inventor accused Nintendo of infringing his patent for use with its 3DS gaming console, shown here.

Following a bench trial, Judge Rakoff ruled in April 2016 that there were substantial differences between the way the Nintendo 3DS produces 3-D images and the process described in the patent. *Tomita Techs. v. Nintendo Co.*, 182 F. Supp. 3d 107 (S.D.N.Y. 2016).

"The differences combine to allow the 3DS to operate more flexibly and to accomplish multiple adjustments at once," the judge wrote.

Tomita's lawyers appealed, arguing Judge Rakoff erred in finding that Nintendo's process isn't covered by the patent. But the Federal Circuit refused to set aside his ruling, finding that it was based on a "comprehensive comparison" of Nintendo's technology and Tomita's patent. WJ

(Reporting by Jan Wolfe)

Attorneys:
Plaintiffs-appellants: Ian DiBernardo, Stroock & Stroock & Lavan, New York; Joseph Diamante and Kenneth Stein, Stroock & Stroock & Lavan, Washington, DC

Defendants-appellees: James S. Blank and Scott G. Lindvall, Arnold & Porter Kaye Scholer, New York, NY; Paul Margulies, Arnold & Porter Kaye Scholer, Washington, DC

Related Filing:
Opinion: 2017 WL 1034471

PUBLIC RECORDS

California city workers' communications on personal accounts not protected from disclosure

By Pauline Toboulidis

California city employees' communications about public business, if made through personal accounts, may be subject to disclosure under the state's Public Records Act, California's highest court has ruled.

City of San Jose et al. v. Superior Court of Santa Clara County et al., No. S218066, 2017 WL 818506 (Cal. Mar. 2, 2017).

In a unanimous decision reversing an appeals court, the state Supreme Court held that city employees' communications about public business are not excluded from the public records law simply because they are sent or received using nongovernment accounts.

> California case law supports the finding that records are subject to disclosure if the agency is in actual or constructive possession of the records, the state high court said.

Without ruling upon a particular search method for responsive documents, the high court remanded the case with some guidance about how to strike a balance between disclosure and employees' privacy.

REQUEST FOR DOCUMENTS

In June 2009 Ted Smith requested the disclosure of several public records from the city of San Jose, its redevelopment agency, and city officials and staff members regarding redevelopment efforts under the California Public Records Act, Cal. Gov't Code § 6250, according to the high court opinion.

The request included emails and text messages of the mayor, City Council members and their staff members from private electronic devices, the opinion said.

In response, San Jose produced communications made using only city telephone numbers and email accounts, according to the opinion.

Smith filed a declaratory action suit arguing that "public records" within CPRA means all communications regardless of where or how they are conducted or stored.

The city responded that communications from employees' personal accounts are not within the city's custody or control and therefore are not public records.

The Santa Clara County Superior Court disagreed and ordered disclosure. The 6th District Court of Appeal issued a writ of mandate preventing the city from complying with the order. *City of San Jose v. Super. Ct.*, 225 Cal. App. 4th 75 (Cal. Ct. App., 6th Dist. 2014).

PUBLIC INTEREST IN GOVERNMENT DISCLOSURE

The California Supreme Court reversed appellate court, holding that documents concerning public business are subject to the CPRA even if they are prepared or transmitted using a personal account.

The CPRA acknowledges a presumptive right to access any record created or maintained by a public agency that relates to the business of that agency, Justice Carol A. Corrigan wrote for the high court.

That right derives from a strong public policy interest in favor of the people's right to information concerning government business, as well as the state's constitutional mandate to construe any limit to the right to access narrowly, the judge said.

PREPARED, OWNED OR RETAINED BY GOVERNMENT AGENCY?

The high court rejected the city's argument that communications through personal accounts are not public records because the CPRA requires that such writings must be "prepared, owned, used, or retained by any state or local agency."

The court also rejected the government's attempt to distinguish CPRA obligations between state and local agencies by arguing the definition of "local agency" does not include individual officers and employees as the "state agency" definition does.

That interpretation does not correlate with the CPRA's broad goal of promoting public access, the high court said.

Communications owned, used or retained by public agencies are subject to the CPRA, regardless of authorship, the court said.

The court also rejected San Jose's argument that because the city did not have direct access to employees' personal accounts, it did not retain the information contained in those accounts.

California case law supports the finding that records are subject to disclosure if the agency is in actual or constructive possession of the records, the high court said.

A contrary holding would thwart the legislative intent to prevent government agencies from avoiding public disclosure by transferring records to a personal account.

The high court recognized that although there are exceptions to public disclosure, an exception is generally applied based on the content of a communication and on a case-by-case basis, not categorically. WJ

Attorneys:
Petitioners: Richard Doyle, Nora Frimann and Margo Laskowska, Office of the City Attorney, San Jose, CA

Related Filing:
Opinion: 2017 WL 818506

INSURANCE

Accounting firm loses forgery, computer fraud coverage appeal

By Melissa J. Sachs

An accounting firm cannot seek coverage from its insurer after an employee relied on emails with instructions, allegedly sent by a client, and transferred nearly $200,000 to foreign bank accounts, a California federal appeals court has affirmed.

Taylor & Lieberman v. Federal Insurance Co., No. 15-56102, 2017 WL 929211 (9th Cir. Mar. 9, 2017).

About half of the money was never recovered, according to filings in the case.

Taylor & Lieberman's policy with Federal Insurance Co. covered losses resulting from forgery of financial instruments, and the emails sent to the accounting firm did not qualify as this type of document, the 9th U.S. Circuit Court of Appeals said.

Under the policy, financial instruments included checks, drafts or similar written promises made by Taylor & Lieberman or an entity purporting to be the accounting firm, the opinion said.

Here, the emails directing the wire transfer came from an unknown perpetrator pretending to be Taylor & Lieberman's client, according to the opinion. This scheme, known as social engineering, relies on communications that appear safe and credible.

But because neither Taylor & Lieberman nor an entity pretending to be the accounting firm drafted the emails, the three-judge panel affirmed the lower court's decision that Federal owed no coverage.

WIRE-TRANSFER INSTRUCTIONS

As part of its business, Taylor & Lieberman holds a power of attorney for clients' financial accounts, according to the firm's complaint against Federal, filed in the U.S. District Court for the Central District of California. *Taylor & Liberman v. Fed. Ins. Co.*, No. 14-cv-3608, *complaint filed* (C.D. Cal. May 9, 2014).

With this power, the accounting firm has the authority to issue payments and transfer funds on its clients' behalf under certain circumstances, the complaint said.

On June 4, 2012, an unknown person obtained control of a client's email account and fraudulently requested that Taylor & Lieberman transfer almost $95,000 to a bank account in Malaysia, the suit said.

The next day, the accounting firm received a second email from the client's address. This email instructed the firm to wire almost $99,000 to a bank account in Singapore, the suit said.

A few days later, the accounting firm received a third email, allegedly from the client, with instructions to wire $128,000 to another Malaysian bank, the suit said.

The third email came from a different email address so Taylor & Lieberman called the client to confirm. It discovered the three requests were fraudulent and did not complete the third transfer, the complaint said.

According to the complaint, the $95,000 was recovered but the $99,000 was stolen.

COVERAGE DISPUTE

At the time of the wire transfers, Federal Insurance had issued a policy to the accounting firm to cover losses from forgery, computer fraud and fraudulent wire transfers, the suit said.

After recouping some money, Taylor & Lieberman submitted a claim to the insurer, which Federal denied, and the accounting firm filed a breach-of-contract suit.

Federal argued it owed no coverage because the policy only covered Taylor & Lieberman for direct losses.

The accounting firm argued it suffered a direct loss when it transferred the client's funds because it held power of attorney and the money was in its control.

Judge Lew agreed with the insurer, saying courts interpret a direct loss to mean a loss that happens immediately without any intervening circumstances.

Here, too many remote circumstances occurred to consider the transfer a direct loss for Taylor & Lieberman, the judge said, granting Federal's summary judgment motion. *Taylor & Lieberman v. Fed. Ins. Co.*, No. 14-cv-3608, 2015 WL 3824130 (C.D. Cal. June 18, 2015).

Taylor & Lieberman appealed to the 9th Circuit, but the appeals court agreed that Federal's policy offered no coverage, despite reaching this conclusion on different grounds.

NOT FORGERY OR COMPUTER FRAUD, 9TH CIRCUIT SAYS

The 9th Circuit said the funds transfer fraud provision in the policy did not cover Taylor & Lieberman's losses because it required the wire transfers to take place without the accounting firm's knowledge.

The appeals court also said the forgery provision did not offer coverage because the emails were not financial instruments.

Taylor & Lieberman's losses resulting from the emailed wire-transfer instructions also did not qualify for coverage under the policy's computer fraud provision, the opinion said.

This provision protected Taylor & Lieberman for losses resulting from unauthorized entries into the accounting firm's computer system, the 9th Circuit said.

Under a "common sense reading" of the policy, this provision was designed to cover losses caused by a perpetrator injecting malware or a virus into the firm's computer system, the 9th Circuit said.

It did not provide coverage when the firm was sent an email with typed out instructions from someone pretending to be a client, the opinion said. WJ

Attorneys:
Appellant: Robert D. Whitney, Edison, McDowell & Hetherington, Oakland, CA; Jeffrey N. Williams and Raymond J. Tittmann, Wargo & French, Los Angeles, CA

Appellee: Gary J. Valeriano and Kenneth Watnick, Anderson, McPharlin & Conners, Los Angeles, CA

Related Filings:
Opinion: 2017 WL 929211
Appellant's reply brief: 2016 WL 2772820
Appellee's brief: 2016 WL 1271920
Appellant's brief: 2016 WL 294077
Complaint: 2014 WL 10190549

DATA BREACH

AshleyMadison.com sued again for 2015 records breach

By Melissa J. Sachs

Another anonymous customer has sued AshleyMadison.com, a "hookup" website for people who are married or in committed relationships, based on a 2015 cyberattack when hackers stole millions of users' personal information and published it online.

Doe v. Avid Life Media Inc., No. BC652729, complaint filed (Cal. Super. Ct., L.A. Cty. Mar. 3, 2017).

An unidentified male filed the lawsuit pro se as "John Doe 312017" in the Los Angeles County Superior Court against Avid Life Media Inc., the Toronto-based company that owns AshleyMadison.com and specialized dating websites CougarLife.com and EstablishedMen.com.

His complaint is similar to other lawsuits filed against the company in Alabama, Texas and California after a hacker or a group of hackers published more than 30 million customers' names, addresses and payment details to the so-called dark web Aug. 18, 2015.

The dark web is an encrypted network for anonymous internet traffic reached through a specialized browser, but other websites republished the data, adding search or filter features, according to an Aug. 19, 2015, article from Wired.

EARLIER LAWSUITS

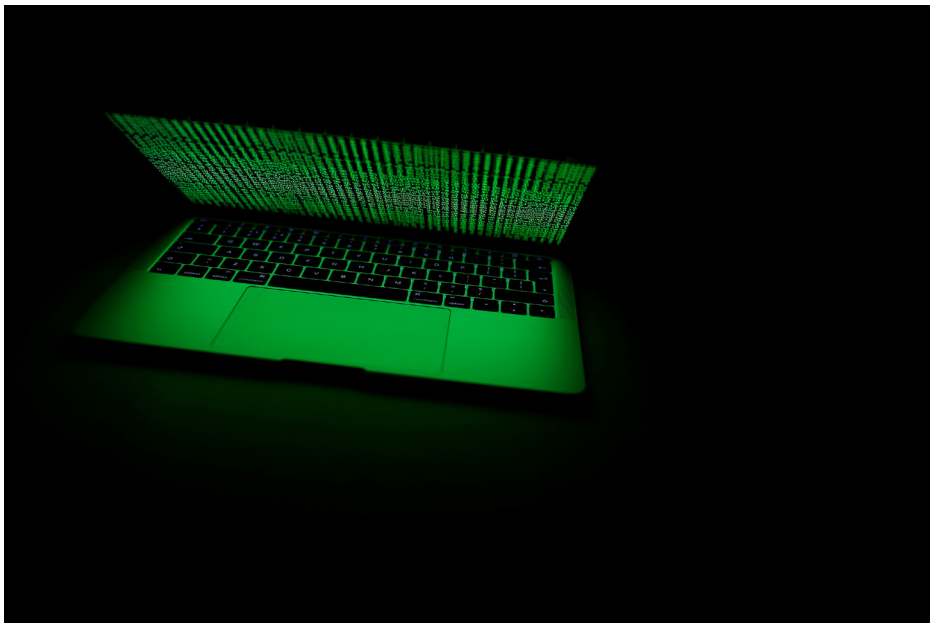
According to the earlier-filed, more detailed lawsuits, a hacker or group of hackers called The Impact Team warned Avid Life in July 2015 that it would leak all customer records if AshleyMadison.com and EstablishedMen.com were not taken offline.

The customer records included descriptions of users' sexual fantasies matched with their payment details, names, addresses and emails, the suits say.

Additionally, The Impact Team threatened to release profiles that Avid Life had promised it would "scrub" from AshleyMadison.com, according to the complaints.

For a $19 fee, Avid Life said it would scrub, or delete, a customer's information from the company's database, but it failed to live up to its promise, the suits allege.

By mid-August 2015, Avid Life had not taken AshleyMadison.com or EstablishedMen.com



REUTERS/Kacper Pempel

offline or notified the potentially affected users about the July hack, according to the suits, which targeted only the leak of Ashley Madison records.

The Impact Team fulfilled its warning and "dumped" the customer information on the web, causing a slew of anonymous individuals to sue Avid Media for negligence and breach of contract related to how it secured customers' sensitive information.

The Judicial Panel on Multidistrict Litigation consolidated and transferred the earlier lawsuits against Avid Media concerning the data dump to Missouri federal court in December 2015.

Earlier this year, U.S. District Judge John A. Ross of the Eastern District of Missouri had scheduled argument for Avid Media's motion to dismiss or stay and compel arbitration for Feb. 17, but he recently postponed the hearing to an unspecified date.

A status conference in that action is scheduled for May 5.

RECENT CALIFORNIA COMPLAINT

Doe 312017's California lawsuit does not mention the pending multidistrict litigation in Missouri.

He alleges Avid Media failed to live up to its security promises and breached its obligations to follow best practices on how to safeguard payment card data.

He also alleges Avid Media failed to use reasonable care to protect customers' sensitive information or mitigate the breach once it received the warning.

The complaint alleges negligence, breach of contract and violation of the Stored Communications Act, 18 U.S.C.A. § 2702.

The plaintiff seeks compensatory and punitive damages, interest and penalties. WJ

Related Filing:
Complaint: 2017 WL 906127

EMPLOYMENT

Oilfield services company may access programmer's software files, court affirms

By Melissa J. Sachs

A computer programmer must let an oilfield services company have access to source code that he developed while working there, a Texas appeals court has affirmed.

Efremov v. GeoSteering LLC, No. 1-16-358-cv, 2017 WL 976072 (Tex. App., 1st Dist. Mar. 14, 2017).

GeoSteering LLC presented a plausible case that programmer Sergey Efremov was a company employee when he developed the source code at issue, the Texas Court of Appeals in Houston said.

Although Efremov maintained he was an independent contractor and owned the intellectual property rights to the software code, there was conflicting evidence about his employment status, the opinion said.

The appeals panel deferred to the trial judge's credibility determinations and upheld the ruling in the company's favor.

It sent the ongoing trade secrets and breach-of-contract suit back to the trial court for further proceedings.

GEOSTEERING'S SOFTWARE

Houston-based GeoSteering LLC offers services to monitor drilling operations using real-time data.

Software called RigComms is the company's main asset, according to the appeals court opinion.

Efremov began working for GeoSteering in 2009. He developed algorithms in one programming language and a GeoSteering engineer would rewrite his code for RigComms in a different programming language, according to the opinion.

At first, Efremov shared access to the algorithms and source code through Dropbox, a file sharing site, the opinion said.

However, in 2015 GeoSteering discovered Efremov had stopped sharing the source code and had removed all files from Dropbox that had not been implemented into RigComms, according to the company.

A QUESTION OF PREEMPTION

GeoSteering sued Efremov in the Fort Bend County 400th District Court, saying he breached his contract and his fiduciary duty to the company and also misappropriated trade secrets.

The trial judge entered a temporary injunction in favor of GeoSteering, finding Efremov was an employee when he developed the source code and other related computer files so they belonged to the company.

Efremov appealed, saying not only that he owned the source code, but also that the trial court had no jurisdiction over GeoSteering's claims because they were preempted by federal copyright law.

The three-judge appeals court panel rejected both arguments.

Section 106 of the Copyright Act, 17 U.S.C.A. § 106, sets forth a copyright owner's exclusive rights, including reproduction, distribution and licensing rights.

It preempts only state law claims that seek to protect equivalent rights, the opinion said.

"GeoSteering's breach-of-contract and breach-of-fiduciary-duty claims turn on whether Efremov was an employee, not on an interpretation of the Copyright Act," the panel said.

EMPLOYEE OR INDEPENDENT CONTRACTOR?

As for whether Efremov was an employee, the panel emphasized that it was reviewing a temporary injunction and so it looked to see only if GeoSteering had a probable right of recovery.

The company showed it had invested significant time training Efremov and gave him all the data to create the algorithms, according to the appeals court's opinion.

Deferring to the discretion of the trial judge, the appeals panel upheld the injunction requiring Efremov to provide GeoSteering with access to the source code and files and preventing him from using, copying or licensing them. WJ

Attorneys:
Appellant: Alexey V. Tarasov, Houston, TX

Appellee: Lionel Martin and Melissa Garcia Martin, Garcia-Martin & Martin, Sugar Land, TX

Related Filings:
Opinion: 2017 WL 976072
Appellee's brief: 2016 WL 6661739
Appellant's brief: 2016 WL 3958881

See Document Section D (P. 39) for the opinion.

ONLINE REVIEWS

Glassdoor fends off forced disclosure of poster's identity

By Jason Seashore, J.D.

Jobs website Glassdoor does not have to reveal the identity of a former software development firm worker who posted a negative review about the company, a California appeals court ruled, reversing a trial court order.

Glassdoor Inc. v. Superior Court of Santa Clara County et al., No. H042824, 2017 WL 944227 (Cal. Ct. App., 6th Dist. Mar. 10, 2017).

Machine Zone Inc. failed to make a prima facie showing that the anonymous review disclosed its confidential information in violation of the nondisclosure agreement signed by all employees, the 6th District Court of Appeal said.

In reversing the lower court, the appellate court said Machine Zone's assertions that the former employee disclosed confidential information were "too vague and conclusory."

'A SCANDAL'

According to the appeals court opinion, the ex-employee posted a review of Machine Zone on Glassdoor Inc.'s website in June 2015 titled "A Scandal," which knocked the company for inflated product claims, a lack of direction from senior management and poor work-life balance for employees.

In July 2015 Machine Zone sued the anonymous poster for breach of contract and won a court order compelling Glassdoor to disclose the person's identity, the opinion said.

Glassdoor petitioned the appeals court for a writ directing the trial court to set aside its order.

As a threshold standing issue, Presiding Justice Conrad Rushing rejected Machine Zone's contention that Glassdoor could not assert the poster's First Amendment right to speak anonymously.

A "substantial preponderance of national authority" favors the rule that publishers may assert the First Amendment interests of their anonymous contributors in maintaining anonymity, and Glassdoor enjoys a "sufficiently close relationship" with the poster to do so, the judge said.

Justice Rushing said that in order to discover the poster's identity, Machine Zone must clearly identify the specific statements the poster made that disclosed confidential information giving rise to his liability.

Machine Zone's entire showing before the lower court consisted of a "conclusory" assertion by one of its in-house attorneys that was "too vague" to satisfy its burden of making a prima facie case, the judge said.

ALLEGED CONFIDENTIAL DISCLOSURES

Justice Rushing explained that Machine Zone "finally identified the statements it claims to be actionable and the confidential information it claims they disclosed," but he said the statements "have not been shown to be capable of bearing the meaning" the company attributed to them.

Machine Zone contended the review disclosed confidential information about its development of RTplatform, "a standalone real-time platform technology that enables the exchange of data between billions of endpoints worldwide virtually simultaneously," the judge said.

But the review's statements about the existence and size of Machine Zone's platform team disclosed only generic, nonsecret information, the opinion said.

The judge also said the poster's quoting of CEO Gabriel Leydon's expectations for the team did not disclose confidential information about the then-unreleased platform technology because the information was inaccurate.

Based on Leydon's alleged comments, the review contended that the platform team was not expected to accomplish anything of substance, which was disproven 10 months later when Machine Zone released RTplatform, the opinion said. WJ

Attorneys:
Petitioner (Glassdoor): William J. Frimel, Seubert French Frimel & Warner LLP, Menlo Park, CA; Rebecca L. Epstein, East Palo Alto, CA

Real-party-in-interest: Michael A. Berta and Sean M. Selegue, Arnold & Porter Kaye Scholer, San Francisco, CA; Sean Morris, Arnold & Porter Kaye Scholer, Los Angeles, CA

Related Filing:
Opinion: 2017 WL 944227

Leapfrog asks judge to toss 'nonsensical' investor suit over VTech merger

Leapfrog Enterprises Inc. says in San Francisco federal court papers that an amended shareholder lawsuit claiming the educational toy maker used a misleading recommendation statement to support its 2016 sale to VTech Holdings Inc. is "nonsensical."

Manger v. Leapfrog Enterprises Inc. et al., No. 16-cv-1161, memo supporting dismissal filed (N.D. Cal. Mar. 8, 2017).

In a memo supporting a motion to dismiss, Leapfrog and former directors say the suit lacks facts showing they falsely portrayed the company as in a "dire" financial condition.

U.S. District Judge William H. Orrick of the Northern District of California dismissed an earlier version of the complaint in January, finding it failed to plead enough facts showing the defendants' alleged statements were false or made with fraudulent intent. *Manger v. Leapfrog Enters.,* No. 16-cv-1161, 2017 WL 282739 (N.D. Cal. Jan. 23, 2017).

Lead plaintiff Pete Manger filed a second amended complaint Feb. 13 that adds "confidential" statements by former Leapfrog employees about the company's optimistic sales forecast for a new children's tablet computer in the 2015 holiday season.

The defendants' memo says the witnesses' statements merely confirm information already disclosed by Leapfrog without showing the company was deceptive about its overall financial condition.

LOOMING LIQUIDITY CRISIS?

Manger filed the original complaint March 9, 2016, less than a week after Leapfrog filed the merger recommendation statement with the U.S. Securities and Exchange Commission.

VTech, a Hong Kong-based toy company, announced April 5 that it had completed its acquisition of Leapfrog through a tender offer that valued the target's shares at $1 apiece.

The recommendation statement allegedly emphasized an unprofitable TV gaming console called LeapTV while omitting any reference to the Epic tablet, an Android-based mobile device released in 2015.

Leapfrog had previously touted Epic's success, saying it was the highest-selling children's tablet during the 2015 holiday season, according to a first amended complaint filed Sept. 6.

The recommendation statement allegedly said there was a "significant possibility" the company would not have sufficient liquidity to operate through the first half of the fiscal year starting April 1, 2016.

Manger also claimed that Leapfrog's directors received a superior offer of $1.10 per share from L&M Acquisitions Inc. on March 24, 2016, but rejected it because the VTech deal offered them personal financial benefits such as accelerated vesting of restricted stock.

AMENDED CLAIMS

The second amended complaint says Barbour stated in a second-quarter earnings call Nov. 9, 2015, that early Epic tablet sales had exceeded expectations and the company was working with retailers to increase their holiday forecast.

During the same call, former Chief Financial Officer Ray Arthur allegedly said Leapfrog could access a $75 million revolving credit facility to fund operations through the fourth quarter, when cash flow was expected to turn positive.

A former Leapfrog senior allocations analyst and a former sales analytics manager confirmed the conference call statements, according to the suit.

The complaint also says Leapfrog's recommendation contradicted its statements to the United Kingdom's Competition and Markets Authority, which evaluated the acquisition for competitive purposes.

The company's CMA filings show it would not have faced a potential liquidity shortfall until June or July 2016, the suit says.

LEAPFROG: DISCLOSURES WERE ACCURATE

In their March 8 memo supporting dismissal, the defendants say the second amended complaint "compounds" the pleading deficiencies that led Judge Orrick's January dismissal.

The suit's falsity allegations "make no sense" because Leapfrog's prediction of a liquidity crisis in the first half of the fiscal year coincides with the CMA's conclusion that the company would have failed financially in June or July 2016, the memo says.

Furthermore, Barbour's and Arthur's remarks in the November 2015 conference call do not demonstrate falsity because they were made prior to the holiday season, the memo says.

The plaintiff "entirely misses" that the recommendation statement disclosed Leapfrog's 2015 holiday sales had fallen $23 million short of expectations, causing the company to lower its 2016 sales forecast, according to the memo.

The defendants say the second amended complaint presents the "exact same scienter theory" Judge Orrick already rejected. It also fails to show that investor losses actually were caused by any misstatement.

The plaintiff's response to the dismissal motion is due March 29. WJ

Related Filing:
Memo: 2017 WL 928386

Class action defense spending topped $2.17 billion in 2016, survey says

By Nicole Banas

Fueled by a spike in high-risk cases, class action defense spending rose to $2.17 billion last year, according to the 2017 Carlton Fields Class Action Survey.

Litigation firm Carlton Fields Jorden Burt P.A. published its sixth annual survey report March 6 based on nearly 400 interviews with senior legal officers or general counsel at about 375 companies nationwide.

The results for 2016 show that defense spending on class actions climbed from $2.1 billion in 2015, following a four-year decline from $2.24 billion in 2010. Expenditures are expected to increase to $2.2 billion in 2017, the report said.

A key takeaway from the survey is that fewer companies reported managing at least one class action, even though respondents perceived an increase in their potential exposure and risk.

The report says companies are increasingly facing potentially catastrophic, "bet the company" cases, which rose from 9.5 percent of class actions in 2015 to more than 25 percent in 2016, the report says.

The report also includes data on defense strategies, risk management and cost reduction measures.

EMPLOYMENT CASES SPIKE

According to the report, labor and employment cases overtook consumer fraud as the most common type of class action, representing nearly 40 percent of suits filed in 2016.

The change is likely related to an upsurge in wage-and-hour suits, particularly in California, the report says.

Consumer fraud cases reportedly constituted 19 percent of class actions, a 6 percent decline from 2015.

The report notes that data privacy actions, which were highly anticipated in recent years, represented less than 5 percent of class actions filed in 2016.

'POLARIZED' RISK

The survey also showed the risk landscape is becoming "more polarized" as the numbers of both high-risk cases and routine class actions increased, the report says.

Carlton Fields said the polarization appears to be affecting defense strategies: Survey respondents increasingly described their company's philosophy as either "defend at all costs" or "go low."

The most commonly reported defense strategy in 2015 was "defend at the right cost."

CASE MANAGEMENT STRATEGIES

According to the report, companies utilize an average of three to four in-house attorneys to manage their class actions.

"Not surprisingly, these in-house attorneys are spending more time on class actions, and their companies are relying more heavily on outside counsel," the report says.

The report says class action settlements decreased from nearly 69 percent in 2015 to 62.5 percent in 2016, with the bulk of settlements occurring prior to class certification.

The use of mandatory arbitration clauses in contracts declined to 30 percent, possibly due to the Consumer Financial Protection Bureau's proposed rule prohibiting the use of class action waivers in some consumer contracts, the report says.

Survey respondents additionally reported a continued reduction in the use of alternative fee arrangements, which are compensation agreements between a law firm and a client based on a structure other than hourly billing. Less than 36 percent of companies used AFAs for class action work, compared to nearly 54 percent in 2014, the report said.

The full report is available at https://www.carltonfields.com/. WJ

CASE AND DOCUMENT INDEX