Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 7 / SEPTEMBER 11, 2015

WHAT'S INSIDE

FIRST AMENDMENT

7 Student's off-campus rap video cause for suspension, full 5th Circuit says

Bell v. Itawamba Cnty. Sch. Bd. (5th Cir.)

COPYRIGHT INFRINGEMENT

8 Suit: Georgia's official code copied, posted online without authorization

Code Revision Comm'n v. Public.Resource.org (N.D. Ga.)

DATA BREACH

9 3rd Circuit permits FTC to continue cybersecurity case against Wyndham

FTC v. Wyndham Worldwide Corp. (3d Cir.)

10 Cheating website Ashley Madison hit with data breach suits

Doe v. Avid Life Media (N.D. Ala.)

11 IRS taxed with data breach suit over 330,000 stolen records

Welborn v. IRS (D.D.C.)

12 Adobe settles data breach suit, will pay $1 million in legal costs

In re Adobe Sys. Privacy Litig. (N.D. Cal.)

CONSUMER FRAUD

13 Symantec to pay $60 million to settle 'download insurance' fraud case

Khoday v. Symantec Corp. (D. Minn.)

MISAPPROPRIATION

14 Video game makers can't intervene in source code suit

Lilith Games (Shanghai) Co. v. uCool Inc. (N.D. Cal.)

CRIMINAL LAW

Prosecutors' anonymous online comments mean mistrial, 5th Circuit affirms

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

Five New Orleans police officers convicted of conspiring to cover up the shooting of six unarmed people in the days following Hurricane Katrina, killing two, deserve a new trial because of prosecutors' anonymous online comments about the case, a federal appellate panel has ruled.

United States v. Bowen et al., No. 13–31078, 2015 WL 4925029 (5th Cir. Aug. 18, 2015).

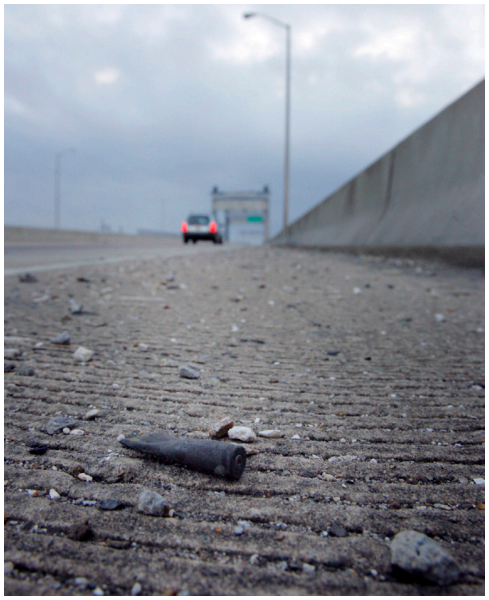
The prosecutorial misconduct, including a botched investigation into the online postings, warranted a new trial for the officers convicted for their involvement in the 2005 events, the 5th U.S. Circuit Court of Appeals said in a 2-1 decision.

Rule 33 of the Federal Rules of Criminal Procedure allows a court to grant a new trial if the "interest of justice so requires," U.S. Circuit Judge Edith H. Jones wrote for the panel's majority.

Based on the record, there was sufficient evidence to show that the inflammatory online postings from federal prosecutors and a Justice Department attorney had a substantial and injurious effect on the outcome in the highly publicized case against the officers, she said.

Judge Jones, joined by Judge Edith Brown Clement, affirmed the lower court's decision to grant a mistrial for these reasons.

CONTINUED ON PAGE 20



REUTERS/Lucas Jackson

A bullet shell lies alongside the road on the Danziger Bridge in New Orleans in this photo taken Nov. 10, 2005. Four police officers convicted on charges related to the shooting deaths of civilians on the bridge in the aftermath of Hurricane Katrina have won a new trial.

COMMENTARY

How to avoid and respond to a cybersecurity breach

With the increase in data breaches occurring at companies and institutions nationwide, Pepper Hamilton LLP attorneys Jan P. Levine, Sharon R. Klein, Angelo A. Stio III and Brian R. Zurich analyze how to navigate through the various state and federal notification laws. They also suggest some corporate strategies for managing risk.

SEE PAGE 3

41737770

Westlaw Journal Computer & Internet

Published since November 1983

Publisher: Mary Ellen Fox

Managing Editor: Robert W. McSherry

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

Managing Desk Editor: Robert W. McSherry

Senior Desk Editor: Jennifer McCreary

Desk Editor: Sydney Pendleton

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

Criminal Law: *United States v. Bowen*
Prosecutors' anonymous online comments mean mistrial, 5th Circuit affirms (5th Cir.) 1

Commentary: By Jan P. Levine, Esq., Sharon R. Klein, Esq., Angelo A. Stio III, Esq., and Brian R. Zurich, Esq., Pepper Hamilton LLP
How to avoid and respond to a cybersecurity breach 3

First Amendment: *Bell v. Itawamba Cnty. Sch. Bd.*
Student's off-campus rap video cause for suspension, full 5th Circuit says (5th Cir.) 7

Copyright Infringement: *Code Revision Comm'n v. Public.Resource.org*
Suit: Georgia's official code copied, posted online without authorization (N.D. Ga.) 8

Data Breach: *FTC v. Wyndham Worldwide Corp.*
3rd Circuit permits FTC to continue cybersecurity case against Wyndham (3d Cir.) 9

Data Breach: *Doe v. Avid Life Media*
Cheating website Ashley Madison hit with data breach suits (N.D. Ala.) 10

Data Breach: *Welborn v. IRS*
IRS taxed with data breach suit over 330,000 stolen records (D.D.C.) 11

Data Breach: *In re Adobe Sys. Privacy Litig.*
Adobe settles data breach suit, will pay $1 million in legal costs (N.D. Cal.) 12

Consumer Fraud: *Khoday v. Symantec Corp.*
Symantec to pay $60 million to settle 'download insurance' fraud case (D. Minn.) 13

Misappropriation: *Lilith Games (Shanghai) Co. v. uCool Inc.*
Video game makers can't intervene in source code suit (N.D. Cal.) 14

Insurance Coverage: *PTC Inc. v. Charter Oak Fire Ins. Co.*
No duty to defend software provider in copyright-extortion suit (D. Mass.) 15

Patents: *Personalized User Model LLP v. Google Inc.*
Google can't get rights to patents for personalizing searches (Fed. Cir.) 16

Patents: *Immersion Corp. v. HTC Corp.*
PTO filings for touch device patents were timely, U.S. and IP owners say (Fed Cir.) 17

News in Brief 18

Presuit Demand/Business Judgment: *Seidl v. Am. Century Cos.*
Mutual fund board rightly rejected suit over Internet gaming investment, 8th Circuit finds (8th Cir.) 19

Case and Document Index 21

How to avoid and respond to a cybersecurity breach

By Jan P. Levine, Esq., Sharon R. Klein, Esq., Angelo A. Stio III, Esq., and Brian R. Zurich, Esq.
Pepper Hamilton LLP

In light of numerous recent data breaches, cybersecurity has emerged as an issue impacting organizations ranging from the local hardware store to the largest multi-national firms in the world. In short, no industry is immune to the threat of a data breach.

While some business sectors have begun to adapt to the changing technological environment, many organizations remain woefully underprepared. According to Verizon's recent Data Breach Investigations Report, in 60 percent of cases, attackers were able to compromise an organization within minutes.[1]

So what can organizations do to prevent or otherwise prepare for a cybersecurity breach? It is imperative to understand where and how your organization stores data and the laws applicable to that data.

This article will focus on the legal framework. As an initial matter, it is important to understand that data security laws vary by industry and state and while there are numerous federal regulations addressing cybersecurity, there is no one uniform law on the subject.

STATE PRIVACY LAWS

The broadest of the cybersecurity regulations are the state data breach notification laws. The state data breach laws are not industry specific and therefore apply to virtually all organizations.

> While some business sectors have begun to adapt to the changing technological environment, many organizations remain woefully underprepared.

In addition to 47 states, the District of Columbia, Puerto Rico, Guam and the Virgin Islands have enacted statutes requiring notification of security breaches involving personal information. Notification is based on the location of the affected individuals, not the location of the breach. Thus, even one small incident could implicate the laws of numerous states. Moreover, organizations must act quickly as notice deadlines range from 10 days after discovery of the incident to "without unreasonable delay."[2]

There is essentially a three-step analysis to determine whether a state law requires notification of a data breach. First, you must examine the law's definition of a breach. Second, you must examine if "personal information" is involved. Third, in some states you must apply an analysis of unauthorized access and risk of harm.

Most state laws generally define a data breach as the unauthorized acquisition or access to personal information in an electronic or computerized format that compromises the data's security, confidentiality or integrity.

Although data breach statutes vary from state to state, personal information generally includes:

An individual's first name, or first initial, and last name *plus* one or more of the following data elements:

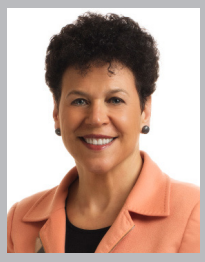
- Social Security number.
- Driver's license or state-issued ID card number.
- Financial or bank account, credit or debit card number *combined with* any security or access code, PIN or password.

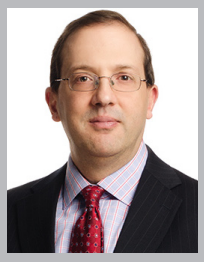
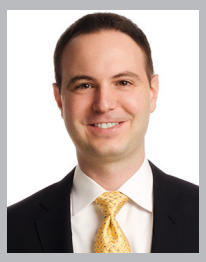
Many states exclude from this definition:

- Any publicly available information that is lawfully made available to the general public from federal, state or local records or widely distributed media.
- Any good-faith access by an employee or agent of the entity for legitimate business purposes only.

Most statutes also include a data-encryption safe harbor, which does not require notification if the compromised data was inaccessible because of encryption.

The final step in the data-breach notification analysis is to see whether the state statute simply requires a showing of unauthorized access or acquisition to trigger notification responsibilities or whether the statute also requires a showing of risk or harm from the unauthorized access or acquisition of the personal information.



(Pictured L-R) **Jan Levine** is a litigation partner and co-chair of the commercial litigation practice group at **Pepper Hamilton LLP**. She is also a member of the firm's privacy, security and data protection group. She can be reached at levinej@pepperlaw.com. **Sharon R. Klein** is a certified information privacy professional (CIPP/US) and the chair of the firm's privacy, security and data protection group and partner-in-charge of its Orange County, Calif., office. She can be reached at kleins@pepperlaw.com. **Angelo A. Stio III** (CIPP/US) is partner in the firm's litigation and dispute resolution department and a member of the firm's privacy, security and data protection group. He can be reached at stioa@pepperlaw.com. **Brian R. Zurich** is an associate in the firm's litigation and dispute resolution department and a member of the firm's privacy, security and data protection group. He can be reached at zurichb@pepperlaw.com.

Several states, as well as the District of Columbia and Puerto Rico, have data breach notification statutes that only require a showing of unauthorized access or acquisition: California, Georgia, Illinois, Minnesota, Nevada, North Dakota and Texas. Generally speaking, all other states incorporate some showing of harm from the unauthorized access or acquisition.

FEDERAL REGULATIONS

There are also numerous mostly industry-focused federal regulations governing cybersecurity.

For example, the Gramm-Leach-Bliley Act applies to financial institutions;[3] the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act apply to the health care industry;[4] and the Family Educational Rights and Privacy Act applies to educational institutions.[5]

Gramm-Leach-Bliley Act

The GLBA, among other things, requires "financial institutions" to develop, implement and maintain administrative, technical and physical safeguards to protect the security, integrity and confidentiality of "nonpublic personal information."[6]

> It is imperative to understand where and how your organization stores data.

"Nonpublic personal information" generally is any information that is not publicly available and that:

- A consumer provides to a financial institution to obtain a product or service.
- Results from a transaction between the consumer and the institution involving a financial product or service.
- A financial institution otherwise obtains about a consumer in connection with providing a product or service.

The term "financial institution" is defined as any business that is significantly engaged in activities that are financial in nature, as well as companies that receive information that is "incidental" or "complementary" to such financial activity. Thus, the definition of financial institution is quite broad.

The GLBA guidelines, which address standards for developing and implementing safeguards to protect customer information, make clear that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer or customers as soon as possible.[7]

This notification guideline under the GLBA is similar to the state notification analysis that requires showing harm or a risk of harm before notification is required.

The Federal Trade Commission enforces the GLBA. While there is no private cause of action under the GLBA, officers and directors of the financial institution can be fined up to $10,000 for each violation, and criminal penalties include imprisonment for up to five years, a fine, or both. Since 2005, the FTC has brought almost 30 cases for violation of the GLBA.[8]

HIPAA and HITECH

The Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, better known as HIPAA and HITECH, set forth privacy and security protections required for the health care industry.

The primary HIPAA/HITECH regulations include the "Standards for Privacy of Individually Identifiable Information," known as the "Privacy Rule," the "Security Standards for the Protection of Electronic Protected Health Information," known as the "Security Rule," and the "Breach Notification Rule."[9]

The Privacy Rule addresses uses and disclosures of "protected health information," or PHI, as well as individuals' rights to access, amend and restrict their PHI and to receive an accounting of their PHI.

Under the Security Rule, covered entities and business associates are required to ensure the confidentiality, integrity and availability of all electronic PHI that the entity creates, receives, maintains or transmits, and to otherwise protect against reasonably anticipated potential breaches, as well as ensuring that their employees comply with the law.

The Breach Notification Rule requires covered entities to provide notification for breaches of unsecured or unencrypted PHI to the affected individuals, the U.S. Department of Health and Human Services, and major print or broadcast media for breaches affecting more than 500 residents of a state or jurisdiction.

> State data breach laws are not industry specific and therefore apply to virtually all organizations.

HHS enforces HIPAA and HITECH through the Office of Civil Rights. HIPAA enforcement actions are usually initiated by a compliant. OCR then conducts an investigation. If the evidence indicates that the entity was not in compliance, OCR will attempt to resolve the case with the covered entity via voluntary compliance. If the entity does not take action to resolve the matter in a way that is satisfactory, OCR may impose a money penalty.

Additionally, following the passage of the HITECH Act, state attorneys general have authority to file civil actions for damages or injunctions in federal courts to enforce HIPAA, and OCR can conduct HIPAA audits.

Generally, there is no private right of action under HIPAA. However, there are examples of state courts ruling that HIPAA's lack of a private right of action does not preclude common law or statutory claims for unauthorized disclosure of medical records. Additionally, state courts have considered HIPAA's standards as the applicable standard of care governing handling of medical records.[10]

Family Educational Rights and Privacy Act

FERPA applies to any public or private elementary, secondary or post-secondary school and any state or local education agency that receives federal funds.[11]

FERPA limits access to a student's education records.

The Family Policy Compliance Office implements FERPA's requirements.

FERPA does not contain specific breach notification requirements. Rather, it protects the confidentiality of education records by

requiring documentation of each disclosure. The federal regulations, nonetheless, encourage direct notification if, for example, the compromised data includes student Social Security numbers or other identifying information that could lead to identity theft.

Similarly, FERPA does not require that an institution notify the Family Policy Compliance Office in the event of a data breach; however, is nonetheless generally considered a best practice to do so.

FERPA does not provide a private cause of action for individuals to sue to enforce the federal funding provisions.

Instead, the Family Policy Compliance Office is responsible to investigate FERPA-related complaints, and federal funds may be withheld from any school or educational agency that fails to comply with the law's regulations.

Other federal law considerations

The GLBA, HIPPA/HITECH and FERPA are far from the only federal laws regulating cybersecurity.

However, they provide basic examples of federal cybersecurity regulations applicable to various organizations.

Other examples of federal regulations include the following:

- The Securities and Exchange Commission's Regulation S-P which generally requires broker-dealers, investment advisers and other financial firms to protect confidential customer information from unauthorized release to unaffiliated third parties.[12]
- The Cable Communications Policy Act of 1984, which regulates the ability of cable operators to collect, disseminate and retain personally identifiable information.[13]
- The Video Privacy Protection Act, which applies to "video tape service providers" and prohibits disclosure of personally identifiable information concerning any consumer.[14]
- The Federal Information Security Modernization Act of 2014, which requires federal agencies and their third-party contractors to develop, implement and comply with certain cybersecurity standards.[15]
- The federal Driver's Privacy Protection Act, which generally prohibits disclosure of any individual's personal information obtained by a department of motor vehicles.[16]
- The Children's Online Privacy Protection Act, or COPPA, which provides online protections for children under 13 years old.[17]
- Several FTC regulations, including Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive practices.[18]
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act, or CAN-SPAM, and the Computer Fraud and Abuse Act.[19]

There are also numerous employment-related statutes that include privacy protections such as the Americans with Disabilities Act, the Family and Medical Leave Act, the Fair Credit Reporting Act, and Title II of the Genetic Information Nondiscrimination Act of 2008.[20]

Most state laws generally define a data breach as the unauthorized acquisition or access to personal information in an electronic or computerized format that compromises the data's security, confidentiality or integrity.

ADDRESSING A DATA BREACH

What should an organization do to address a breach in light of state and federal privacy regulations?

As a threshold matter, the best time for addressing a data breach or cyberattack is before the breach occurs. By having robust policies and procedures in place, together with a response team and appropriate training, organizations will be armed for data breaches and cyberattacks that are now commonplace.

Among other things, organizations should review their insurance coverage. Many providers now offer cyberinsurance coverage and officers and directors may be covered by a directors and officers policy for decisions related to a data breach.

In the event of a cybersecurity breach, however, there is no one-size-fits-all approach. Nonetheless, taking the following actions will help to address most state and federal regulations:

- Gather information and determine what types of data were compromised, including whether the information was encrypted, which may require external computer forensic assistance.
- Determine whether notice is necessary, which in some instances may require a risk-of-harm analysis and the assistance of outside legal counsel.
- Decide who needs to be notified, such as individuals affected, law enforcement (*e.g.*, local police or state attorneys general), consumer reporting agencies (usually only if more than 1,000 individuals are implicated), or government regulators.
- Determine when notice must be provided, usually in the most expeditious time possible to provide an accurate notice and without unreasonable delay, but, in Puerto Rico for example, within 10 days after the violation is detected.
- Draft and send the necessary notices.

CONCLUSION

It is not a question of whether your organization will suffer a cyberbreach, but when. Organizations that understand what information is collected and maintained, the purpose of collecting and maintaining such information, the individuals that have access to it, the security measures that protect the information, and the laws and regulations that apply to the information are far better prepared to reduce the risks associated with cyberbreaches and to more effectively take appropriate action when a breach occurs. As outlined above, the time to plan for a cyberbreach is before the breach occurs by developing policies and procedures, implementing and monitoring security systems, conducting breach roundtables to test preparedness and having a team in place ready to mobilize when that cyberbreach ultimately occurs. WJ

NOTES

[1] *See* Verizon Enter. Solutions, *2015 Data Breach Investigations Report (2015),* http://vz.to/1K2pCSp

[2] Generally, the outside limit under federal legislation, *e.g.*, under HIPAA, is 60 days.

[3] 15 U.S.C. §§ 6801-09.

[4] Pub. L. Nos. 104-191 & 111-5, § 13402.

[5] 20 U.S.C. § 1232g.

[6] 15 U.S.C. § 6801(a).

[7] *See* 12 C.F.R. Pt. 364, App. A.

[8] Fed. Trade Comm'n, Federal Trade Commission 2013 Privacy and Data Security Update, *available at* http://1.usa.gov/1O3YgNB.

[9] *See* 45 C.F.R. Pts. 160, 162 & 164.

[10] *See* Sharon R. Klein, Jan P. Levin, Rebekah A.Z. Monson and Angelo A. Stio III, *Connecticut Supreme Court Allows Plaintiffs to Circumvent HIPAA's No Private Right of Action Clause,* PEPPER HAMILTON LLP CLIENT ALERT (Nov. 25, 2014), *available at* http://bit.ly/1Q42rKD.

[11] The statute's regulations are available at 34 C.F.R. Pt. 99.

[12] 17 C.F.R. Pt. 248.

[13] 47 U.S.C. § 521.

[14] 18 U.S.C. § 2710.

[15] 44 U.S.C. § 3551.

[16] 18 U.S.C. § 2721.

[17] 7 U.S.C. § 231.

[18] 15 U.S.C. §§ 41-51.

[19] 15 U.S.C. § 7701 & 18 U.S.C. § 1030.

[20] 42 U.S.C. § 12101; 29 U.S.C. § 2601; 15 U.S.C. § 1681; & 42 U.S.C. § 2000ff.

Student's off-campus rap video cause for suspension, full 5th Circuit says

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

A Mississippi high school could suspend and transfer a senior after he publicly posted a rap video online that allegedly threatened athletic coaches and warned them to watch their backs, a full federal appeals court has ruled.

Bell et al. v. Itawamba County School Board et al., No. 12–60264, 2015 WL 4979135 (5th Cir. Aug. 20, 2015).

The Itawamba County School Board did not violate Taylor Bell's free-speech rights when it disciplined him for posting his rap video online, a majority of 5th U.S. Circuit Court of Appeals judges decided in a 12-4 *en banc* opinion overturning an earlier ruling by a three-judge panel of the court.

It did not matter if Bell recorded the video off-campus during non-school hours because the rap harassed, intimidated and threatened two school coaches, U.S. Circuit Judge Rhesa H. Barksdale wrote on behalf of the majority.

THE PANEL RULING

A 5th Circuit panel held last December that the school board had violated Bell's First Amendment rights.

> It did not matter if the student recorded the video off-campus during non-school hours because the rap harassed, intimidated and threatened two public school coaches, the majority opinion said.

In a 2-1 decision, the panel found the board never showed that Bell's off-campus video "substantially disrupted" school work or discipline. *Bell et al. v. Itawamba Cnty. Sch. Bd. et al.*, 774 F.3d 280 (5th Cir. 2014) (see *Westlaw Journal Computer & Internet*, Vol. 32, Iss. 17, 32 No. 17 WJCOMPI 4).

The substantial-disruption test comes from *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969), a U.S. Supreme Court case that involved students' free speech rights in school.

The panel majority, Judges James L. Dennis and James E. Graves Jr., said they were not certain the school could rely on the substantial-disruption test to restrict Bell's off-campus speech, which warranted more constitutional protection.

Judge Barksdale was the dissenter on the panel. He expressed concern with Bell's lyrics, especially given the history of school shootings.

After the rehearing by the entire court, Judges Dennis and Graves were in the minority.

"[T]he majority opinion allows schools to police their students' Internet expression anytime and anywhere — an unprecedented and unnecessary intrusion on students' rights," Judge Dennis wrote in his dissent.

Judges Edward C. Prado and Catharina Haynes also wrote dissenting opinions.

THE RAP

According to the opinion, Bell was a senior at Itawamba Agricultural High School and an aspiring rapper when he recorded a song over Christmas break in 2010, which claimed that two male coaches at the school sexually harassed female students. The video also referred to "capping," or shooting, one of the coaches and included a racially derogatory term.

He posted the video on his Facebook page and a second, edited version of the video on YouTube.

When Bell returned to school in January 2011, school officials watched the video, and the superintendent set up a disciplinary hearing, the opinion said.

At the hearing, Bell said he thought his lyrics might bring attention to the problem of teacher-on-student harassment, which he claimed school officials had ignored in the past, the opinion said.

Bell was suspended and transferred to another school for threatening school officials. He sued the school district, principal and superintendent in the U.S. District Court for the Northern District of Mississippi for civil rights violations in February 2011.

The District Court ruled in the defendants' favor.

On appeal before the three-judge panel, two judges rejected the school district's arguments that Bell's off-campus speech caused substantial disruption, finding no evidence in the record to support the argument.

The school board asked for an *en banc* review, which the 5th Circuit granted in February, and the full court overturned the panel's decision.

MORE GUIDANCE

In a concurring opinion, Judge Gregg Costa reflected on how the schools need more guidance on off-campus versus on-campus speech and how to balance a student's First Amendment rights in the digital age.

"That task will not be easy in light of the pervasive use of social media among students and the disruptive effect on learning that such speech can have when it is directed at fellow students and educators," he wrote.

It needs to come soon, however, he said. WJ

Attorneys:
Plaintiffs-appellants: Wilbur O. Colom and Scott W. Colom, Colom Law Firm, Columbus, Miss.

Defendants-appellees: Benjamin E. Griffith, Griffith Law Firm, Oxford, Miss.

Related Court Document:
Opinion: 2015 WL 4979135

Suit: Georgia's official code copied, posted online without authorization

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

A public resource website has until Sept. 14 to answer an Atlanta federal lawsuit alleging it copied an annotated version of Georgia's statutes without authorization and encouraged others to create other unauthorized, derivative works.

Code Revision Commission et al. v. Public.Resource.org Inc., No. 1:15-cv-02594, complaint filed (N.D. Ga., Atlanta Div. July 21, 2015).

The Code Revision Commission filed its copyright infringement lawsuit on behalf of the state and the General Assembly against Public.Resource.org Inc. in the U.S. District Court for the Northern District of Georgia on July 31.

Without authorization, Public.Resource.org copied at least 140 different volumes or supplements of the Official Code of Georgia Annotated, or the O.C.G.A., containing copyrighted annotations of the laws, the complaint says.

Public.Resource.org then published these online, making them widely available to the public, the suit says.

The copyrighted annotations contain summaries of cases interpreting the laws, opinions from the state's attorney general and original research, the complaint says.

The suit does not allege the plaintiff owns a copyright to the O.C.G.A.'s statutory text because Georgia's laws are free to the public and available online at www.legis.ga.gov.

"These free Code publications are available 24 hours each day, 7 days a week and include all statutory text and numbering; numbers of titles, chapters, articles, parts and subparts; captions and headings; and history lines," the complaint says.

Public.Resource.org, however, unlawfully copies the copyrighted annotations to the O.C.G.A., and posts these online, the suit says.

Carl Malamud, founder and president of **Public.Resource.org**, disputes the commission's claims.

"Every bill passed by the Georgia General Assembly begins with the words, 'An Act ... to amend the Official Code of Georgia Annotated,'" he wrote in an email. "The so-called 'free' site provided by the General Assembly comes with stringent terms of use and is explicitly unofficial."

COPYRIGHTED CODE ANNOTATIONS

According to the complaint, the commission helps the Georgia General Assembly compile and obtain the O.C.G.A.

The commission is made up of 15 members from Georgia's house and senate and the state bar, including one superior court judge and a district attorney.

With the commission's assistance, Georgia's Legislature contracts with a third-party publisher — currently, Matthew Bender & Co., a member of the LexisNexis Group — to create this original work as a work-for-hire, the suit says.

To allow LexisNexis to recoup its publishing costs, the state allows it to sell the copyrighted annotated code electronically and in book form, the complaint says.

Kirk Walter

"The so-called 'free' site provided by the General Assembly comes with stringent terms of use and is explicitly unofficial," Public.Resource.org founder and President Carl Malamud said.

LexisNexis will not be able to recoup its costs and the Legislature will have to pass on the costs to tax payers if the federal court does not enjoin Public.Resource.org's unauthorized copying, the suit says.

Public.Resource.org is based in California, but the Atlanta federal court has jurisdiction over the case because the defendant has directed its unlawful activities to the state, the suit says.

Public.Resource.org gave unauthorized copies of the annotated code to state house representatives in May 2013 and, four months later, gave eight more copies to in-state institutions on thumb drives, the suit says.

Additionally, the corporation directs its websites to Georgia citizens, including fundraising platforms seeking to raise money to defend copyright infringement lawsuits, the complaint says.

The suit includes counts for direct and indirect infringement under Section 106 of the Copyright Act, 17 U.S.C. § 106.

It seeks permanent injunctive relief, a court order to seize all infringing works from Public.Resource.org, attorney fees, costs and other proper relief.

Responding to the lawsuit, Malamud says Public.Resource.org is confident it will prevail.

"In the United States, citizens have the right to read and speak the law to inform their fellow citizens, and that is what Public.Resource.org did," he said. WJ

Attorneys:
Plaintiff: Anthony B. Askew, Lisa C. Pavento and Warren Thomas, Meunier Carlin & Curfman, Atlanta

Related Court Document:
Complaint: 2015 WL 4999975

3rd Circuit permits FTC to continue cybersecurity case against Wyndham

By Pamela Park, Senior Attorney Editor, Westlaw Daily Briefing

The 3rd U.S. Court of Appeals has affirmed a district court holding that allowed the Federal Trade Commission's case against Wyndham Worldwide Corp., which concerned Wyndham's cybersecurity practices, to proceed.

Federal Trade Commission v. Wyndham Worldwide Corp., No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015).

The FTC filed suit against Wyndham in 2012 relating to three instances in which hackers gained access to the hotel chain's computer system and stole personal and financial information from hundreds of thousands of customers during 2008 and 2009.

According to the FTC, Wyndham "engaged in unfair cybersecurity practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."

In particular, the FTC noted that Wyndham:

- Permitted hotels to store payment information in clear readable text.
- Allowed the use of easily guessed passwords to access the property management system.
- Failed to use "readily available security measures," such as firewalls, to limit access between its systems.
- Failed to employ "reasonable measures to detect and prevent unauthorized access" to its computer network or to "conduct security investigations."

The FTC's suit claimed that Wyndham engaged in "unfair" and "deceptive" practices in violation of 15 U.S.C. § 45(a).

Wyndham filed a motion to dismiss the FTC's action, which the U.S. District Court for the District of New Jersey denied. However, the court certified its decision on the unfairness claim for interlocutory appeal.

THREE-PRONGED UNFAIRNESS TEST

Citing a 1980 policy statement issued by the FTC, 3rd Circuit noted that the commission clarified that the injury must satisfy three tests in order to justify a finding of unfairness. Congress later codified the FTC's three-pronged test in 15 U.S.C. § 45(n).

According to the test, the injury must be substantial, must not be outweighed by any countervailing benefits to consumers or competition that the practice produces, and must be an injury that consumers themselves could not reasonably have avoided.

The 3rd Circuit was unpersuaded by Wyndham's argument that the plain meaning of the word "unfair" does not support the FTC's case. Countering the company's argument that unfairness means it is not equitable, the court pointed to several of Wyndham's actions that it did not consider "equitable."

The court noted, for example, that a company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy and then fails to make good on that promise, exposing its customers to financial injury.

REUTERS/Gary Cameron

> The 3rd Circuit's decision paves the way for the FTC to prosecute more companies that fail to adequately secure their technology systems.

Wyndham also argued on appeal that, notwithstanding whether its conduct was unfair under Section 45, the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow.

The court held that the relevant question is not whether Wyndham was entitled to know with "ascertainable certainty" the FTC's interpretation of what cybersecurity practices are statutorily required, but whether the company had fair notice that its conduct could fall within the meaning of the statute.

The Wyndham case has been closely watched, as regulators and the public seek to hold companies responsible for cyberbreaches. The 3rd Circuit's decision paves the way for the FTC to prosecute more companies that fail to adequately secure their technology systems. WJ

Attorneys:
Appellants: Kenneth W. Allen, Eugene F. Assaf, Christopher Landau, Susan M. Davies and Michael W. McConnell, Esquire, Kirkland & Ellis, Washington

Appellee: General Counsel Jonathan E. Nuechterlein, Principal Deputy General Counsel David C. Shonka Sr., Director of Litigation Joel R. Marcus and David L. Sieradzki, Federal Trade Commission, Washington

Related Court Document:
Opinion: 2015 WL 4998121

Cheating website Ashley Madison hit with data breach suits

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

Anonymous customers have sued AshleyMadison.com, a hook-up website for people who are married or committed relationships, in three states after hackers stole personal information about millions of users and published it online.

Doe v. Avid Life Media Inc. et al., No. 6:15-cv-01464, complaint filed (N.D. Ala. Aug. 25, 2015).

Doe 1 et al. v. Avid Life Media Inc. et al., No. 8:15-cv-01347, complaint filed (C.D. Cal., Santa Ana Aug. 24, 2015)

Doe v. Avid Life Media Inc. et al., No. 2:15-cv-06405, complaint filed (C.D. Cal., L.A. Aug. 21, 2015).

Doe v. Avid Life Media Inc., No. 3:15-cv-2750, complaint filed (N.D. Tex., Dallas Aug. 21, 2015).

Despite Ashley Madison's promised security measures, a group of hackers published more than 30 million customers' names, addresses and payment details online Aug. 18, according to a proposed class action filed in Alabama federal court against Avid Life Media Inc.

The Toronto-based company owns AshleyMadison.com and specialized dating websites CougarLife.com and EstablishedMen.com.

According to Avid Life's website, EstablishedMen.com "connects ambitious and attractive young women with successful and generous benefactors to fulfill their lifestyle needs."

Other "John Doe" Ashley Madison customers have also filed proposed class actions against Avid Life in federal courts in Los Angeles and Santa Ana, Calif., as well as Dallas.

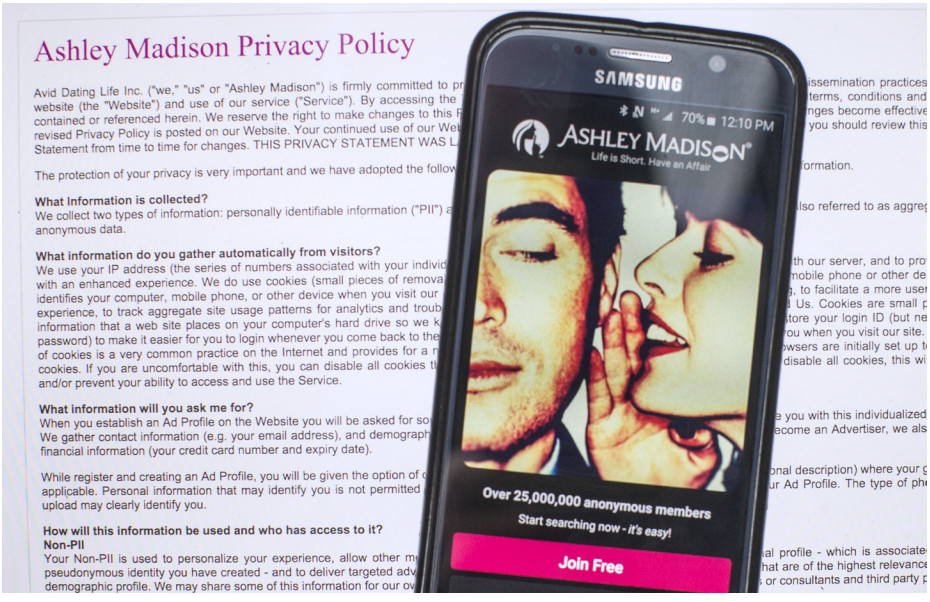
Each complaint seeks over $5 million in damages for the site's alleged negligence in safeguarding users' information.

Avid Media is offering a $500,000 reward for information about the data breach.

The company did not respond to a request for comment on the suit.

CHEATERS HACKED

In late July, a hacker or group of hackers called The Impact Team warned Avid Life that if it did not take AshleyMadison.com and EstablishedMen.com offline, it would leak all customer records, according to the complaints.



REUTERS/Mark Blinch

A photo illustration shows the privacy policy of AshleyMadison.com seen behind a smartphone running the Ashley Madison app. The adultery-promoting website is facing several lawsuits after hackers published more than 30 million customers' names, addresses and payment details online Aug. 18.

The 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 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 has failed to live up to its promise, the suits allege.

Avid Life did not take AshleyMadison.com and EstablishedMen.com offline or notify the potentially affected users about the July hack, according to the suits, which target only the leak of Ashley Madison records.

On Aug. 18, The Impact Team posted data about 37 million Ashley Madison users to the so-called dark Web, an encrypted network for anonymous Internet traffic reached through a specialized browser, the complaints say.

Other websites republished the data, adding search or filter features, according to the complaints and an Aug. 19 article published by Wired.

The information "dumped" on the Web also included some users' photographs, one lawsuit alleges.

CLASS CLAIMS

The lawsuits all include counts for negligence and breach of contract.

Both California suits also allege violations of the state's Customer Records Act, Cal. Civ. Code § 1798.81.5, and public disclosure of private facts.

The Los Angeles suit includes counts for violations of California's common law and the unfair-competition statute, Cal. Bus. & Prof. Code § 17200.

"Needless to say, this dumping of sensitive personal and financial information is bound to have catastrophic effects on the lives of the website's users," the complaint says.

According to the Santa Ana suit, Avid Life also violated various state data breach notification and consumer protection laws.

It seeks injunctive relief ordering third-party security audits and testing, as well as internal training on identifying and responding to data breaches.

In Dallas and Alabama, the federal lawsuits allege Avid Life violated the federal Stored Communications Act, 18 U.S.C. § 2702.

Specifically, the suits say the company failed to take commercially reasonable steps to safeguard customers' private financial information that it maintained on its remote computing service for payment verification purposes.

The Dallas complaint also includes counts for violations of the Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Comm. Code § 17.45(4), and Identity Theft Enforcement Protection Act, Tex. Bus. & Comm. Code § 521.152.

It further includes a count for intentional infliction of emotional distress under the state's common law.

Despite the hackers' warning, Avid Life intentionally or recklessly failed to mitigate the breach, which caused millions of users' private information to be disclosed, the suit says.

The Alabama suit includes a count for violations of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, and fraud or misrepresentation. WJ

Attorneys:
Plaintiff (Alabama): Thomas E. Baddley Jr., Jeffrey P. Mauro and John Parker Yates, Baddley & Mauro, Birmingham, Ala.

Related Court Documents:
Alabama complaint: 2015 WL 5023966
Santa Ana complaint: 2015 WL 5012608
Los Angeles complaint: 2015 WL 4999969

DATA BREACH

IRS taxed with data breach suit over 330,000 stolen records

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

The IRS knew its computer system was vulnerable to hackers but still failed to protect the personal information of more than 330,000 U.S. taxpayers who have had their data stolen since March, according to a federal lawsuit.

Welborn et al. v. Internal Revenue Service et al., No. 1:15-cv-01352, complaint filed (D.D.C. Aug. 20, 2015).

Plaintiffs Becky Welborn and Wendy Windrich are two of the taxpayers who had their personal information stolen through the agency's "Get Transcript" application, according to the complaint filed in the U.S. District Court for the District of Columbia.

The online app allowed taxpayers to access and request copies of their tax returns and other filings.

Because of the app's lax security measures, however, criminals were able to bypass the security questions using personal data scraped from the Web or obtained through other data hacks, according to the complaint.

The app used so-called knowledge-based authentication, giving users challenge questions about past addresses or their mothers' maiden names — information easily found on popular websites such as Zillow, Spokeo and Facebook, the suit says.

The IRS shut down the "Get Transcript" app in May. At that time, hackers had gained unauthorized access to 100,000 tax accounts through the app, a number that rose to 220,000 by August, according to an Aug. 17 agency statement.

Hackers also tried to access data for 170,000 other households, but failed, the statement said.

"The IRS takes the security of taxpayer data extremely seriously, and we are working aggressively to protect affected taxpayers and continue to strengthen our systems," the agency said.

Jason Beach, who handles privacy matters at **Hunton & Williams** in Atlanta but is not involved with this case, said the suit against the IRS shows how cybercriminals do not target only corporations.

"Although many consumers tend to think corporations are the biggest risk for data breaches, the IRS breach reaffirms that government entities are not immune," he said.

WELBORN'S EXPERIENCE

Welborn sent her tax return April 15 in paper form, according to the complaint.

After 10 weeks, when she had not received her refund, she contacted the IRS, the complaint says.

She was on the phone for two hours before an IRS representative told her that someone

Data breaches and Article III standing

Many of the plaintiffs' injury allegations in the IRS litigation are the standard factual fodder that has not been successful in the majority of prior data breach cases.

However, expect any briefing in support of Article III standing to take full advantage of the recent — and plaintiff-favorable — decision by the 7th U.S. Circuit Court of Appeals regarding future injury. *Remijas et al. v. Neiman Marcus Grp. LLC*, No. 14-3122, 2015 WL 4394814 (7th Cir. July 20, 2015)

The most injury-in-fact traction likely will be from the two named plaintiffs' allegations of actual fraud.

— Jason M. Beach, Hunton & Williams

had filed a duplicate joint return using her and her husband's Social Security numbers, the suit says.

The representative said the person had requested past filings through the "Get Transcript" app, according to the complaint.

The agency never contacted Welborn about the unauthorized request and she has not received any notification about the hacks to the "Get Transcript" app, the complaint says.

Welborn says she has spent hours changing her bank account numbers, filing reports with the police and the Federal Trade Commission, requesting fraud alerts from three credit reporting agencies, and submitting an affidavit to the IRS.

WINDRICH'S EXPERIENCE

The IRS contacted Windrich in June, saying it had processed her and her husband's e-filing and electronically deposited $9,300 in the bank account they had provided, the complaint says.

Windrich contacted the IRS to alert it about possible fraud, because she and her husband had asked for an extension. Additionally, for many years, they did not receive a refund, but instead owed taxes, the complaint says.

An IRS representative told Windrich the fraudulent tax return had specific information about her and her family that someone could have only known about from the agency's "Get Transcript" application, the complaint says.

CLASS ALLEGATIONS

The IRS told Welborn and Windrich they will not be able to electronically file their taxes for the foreseeable future, according to the suit.

Additionally, both plaintiffs and their families are at greater risk of identity theft and will need to continuously monitor their accounts, the complaint says.

The suit includes counts for violations of the Privacy Act of 1974, 5 U.S.C. § 552(a), which requires government agencies to establish appropriate safeguards to protect records they collect, and the Administrative Procedure Act, 5 U.S.C. § 701.

The plaintiffs seek class status, actual and statutory damages, injunctive and declaratory relief, costs, fees and interest. WJ

Attorney:
Plaintiffs: Steven W. Teppler, Abbott Law Group, Jacksonville, Fla.

Related Court Document:
Complaint: 2015 WL 5011337

DATA BREACH

Adobe settles data breach suit, will pay $1 million in legal costs

By Jason Schossler, Contributor, Westlaw Journals

A lawsuit alleging Adobe Systems' "lax security measures" resulted in a massive data breach that affected 38 million people has drawn to a close after the company agreed to implement a series of undisclosed protocols to protect its customers' information.

In re Adobe Systems Inc. Privacy Litigation, No. 5:13-cv-05226, motion for approval of voluntary dismissal granted (N.D. Cal., San Jose Div. Aug. 14, 2015).

U.S. District Judge Lucy Koh of the Northern District of California granted the plaintiffs' motion for voluntary dismissal of the consolidated class-action suit nearly two months after the parties announced they had reached an agreement.

The agreement calls for Adobe to use specific security measures that will enhance its network and information security practices. The company also will pay service awards of $5,000 to each of the six named plaintiffs.

In a separate order issued Aug. 13, Judge Koh granted the plaintiffs' motion for attorney fees, ordering Adobe to pay nearly $1.1 million. She found the amount reasonable based on the estimated 2,539 hours plaintiffs' counsel spent working on the case.

SECURITY BREACH

According to the complaint, sometime in mid-July 2013 hackers gained access to Adobe's source code repository and the network that handled credit card transactions. The company failed to warn customers about the extent of the security breach until weeks later, the complaint alleged.

Additionally, Adobe failed to provide customers with adequate identity and credit monitoring services within a reasonable amount of time after the breach, the suit said.

The suit also said Adobe knew its security practices did not meet reasonable industry standards but falsely told the public that they did, causing the plaintiffs and others to pay higher prices for less valuable products.

The suit alleged violations of California's unfair-competition law, Cal. Bus. & Prof. Code § 17200, and data breach statute, Cal. Civ. Code § 1798.80.

ACTUAL INJURY

In September 2014 Judge Koh denied Adobe's bid to dismiss the suit. The company contended the plaintiffs lacked standing because they could not show an actual injury.

The judge disagreed, saying the danger that the plaintiffs' stolen data will be subject to misuse could be reasonably described as "certainly impending."

"The threatened injury here could be more imminent only if plaintiffs could allege that their stolen personal information had already been misused," Judge Koh wrote.

To require the plaintiffs to wait until they actually suffer credit card fraud or identity theft in order to establish standing "would run counter to the well-established principle that harm need not have already occurred ... in order to constitute injury-in-fact," she said.

As part of the settlement agreement, Adobe will submit to a one-time, independent audit to confirm it has successfully implemented new security measures. The audit will be conducted one year from the final settlement date. WJ

Related Court Documents:
September 2014 order: 66 F. Supp. 3d 1197
Consolidated class-action complaint: 2014 WL 1841156

Symantec to pay $60 million to settle 'download insurance' fraud case

By Jason Schossler, Contributor, Westlaw Journals

Two consumers are asking a Minnesota federal judge to preliminarily approve a $60 million settlement of a lawsuit alleging Symantec Corp. misled customers into buying an unnecessary "download insurance" add-on to its Norton Antivirus software package.

Khoday et al. v. Symantec Corp. et al., No. 11-0180, motion for preliminary settlement approval filed (D. Minn. Aug. 18, 2015).

Devi Khoday and Danise Townsend say in a memo filed in the U.S. District Court for the District of Minnesota that the deal will resolve their class-action claims that Symantec and co-defendant Digital River Inc., an online retailer, violated Minnesota's Consumer Fraud Act, Minn. Stat. § 325F.67, and other federal and state laws.

Each member of the plaintiffs' proposed class of Symantec customers who submits a claim will receive about $50 for every purchase of the insurance add-on, according to the memo.

The $60 million sum includes an incentive payment of up to $10,000 each to Khoday and Townsend, the memo said.

The agreement came about five months after U.S. District Judge John R. Tunheim denied Symantec's motion for summary judgment.

In a March 19 ruling, the judge said a genuine fact issue exists as to whether the California-based company misrepresented the need for the insurance. *Khoday et al. v. Symantec Corp. et al.*, No. 11-0180, 2015 WL 1275323 (D. Minn. Mar. 19, 2015) (see *Westlaw Journal Computer & Internet*, Vol. 33, Iss. 2, 33 No. 2 WJCOMPI 7).

NORTON DOWNLOAD INSURANCE

According to the suit, Symantec automatically added "download insurance" to the virtual shopping carts of customers who bought the antivirus software over the Internet between 2005 and 2011.

The insurance, which cost between $4.99 and $16.99, allegedly gave customers the ability to re-download the software after the first 60 days after the purchase. To refrain from buying the insurance, a customer had to affirmatively "opt out" of the purchase and remove it from the shopping cart, the suit said.

Khoday and Townsend said they purchased the insurance believing it was necessary if they wished to re-download the software. However, there were multiple alternative options for customers to re-download the software at no cost through both a customer support website and trialware, according to the suit.

The plaintiffs alleged they were deceived and would not have purchased the insurance had they known there were other re-download options.

In its summary judgment motion, Symantec said the plaintiffs failed to show it made any material misrepresentations or omissions because none of the alternative options were guaranteed to be available for customers to re-download the software.

Judge Tunheim ruled Symantec may prove to be correct in that the insurance was the only "guaranteed re-download option" and that the company had the right to revoke any alternative options.

But a genuine fact issue remained as to whether Symantec had an obligation to disclose the other available options, he said.

Judge Tunheim also rejected Symantec's argument that the plaintiffs suffered no economic loss because the benefit they sought — a guarantee that they would be able to re-download the software beyond 60 days — is exactly what they received.

"A plaintiff may prove detrimental reliance on a material omission and recover damages if, 'had the omitted information been disclosed, [the plaintiff] would have been aware of it and behaved differently,'" he said, citing *Mirkin v. Wasserman*, 5 Cal.4th 1082 (Cal. 1993).

> Prior to the final approval of the agreement, the plaintiffs will request a court order authorizing payment of about $19.8 million in litigation costs, according to the memo.

AN 'EXCELLENT RESOLUTION'

In their memo seeking approval of the settlement, the plaintiffs call the deal "fair, reasonable and adequate" and "an excellent resolution of the litigation."

The settlement will confer a significant benefit on the class and also avoids the "considerable risks, delays and expense inherent in complex class-action litigation," they say.

The plaintiffs also say the deal is the result of "serious, non-collusive, arm's-length negotiations."

Before the final approval of the agreement, the plaintiffs will request an order authorizing payment of about $19.8 million in litigation costs, according to the memo. WJ

Related Court Document:
Complaint: 2011 WL 334412

Video game makers can't intervene in source code suit

By Jason Schossler, Contributor, Westlaw Journals

A San Francisco federal judge has refused to allow the developers of the World of Warcraft" and "Dota 2" video game series to intervene in a source code dispute between fellow developers.

Lilith Games (Shanghai) Co. v. uCool Inc. et al., No. 3:15-cv-01267, 2015 WL 4914694 (N.D. Cal. Aug. 17, 2015).

The lawsuit by Shangai-based Lilith Games Co. alleges uCool Inc. stole its software code to create a nearly identical version of its game "Sword and Tower."

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

> Intervention at this stage would unduly delay resolution of the original parties' infringement case, the judge said.

Fellow developers Blizzard Entertainment Inc. and Valve Corp. moved to intervene in the suit, alleging both Lilith and uCool copied various character and visual elements from their games "World of Warcraft," "Warcraft III," "Diablo III" and "Dota 2."

Rejecting the motion, U.S. District Judge Samuel Conti said in an Aug. 17 order that Blizzard and Valve do not have a "significant protectable interest" related to Lilith's claims.

Even if they did, that interest "would not be impaired by the outcome of this action," he said.

According to the suit, 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 suit alleged 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 said.

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

In July Judge Conti ruled Lilith adequately pleaded facts showing uCool misappropriated its source code in violation of California's Uniform Trade Secrets Act, Cal. Civ. Code § 3426.

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 July 8 order (see *Westlaw Journal Computer & Internet*, Vol. 33, Iss. 5, 33 No. 5 WJCOMPI 11).

PROTECTABLE INTERESTS

In his latest Aug. 17 ruling, Judge Conti said Blizzard and Valve cannot file a complaint-in-intervention for copyright infringement because the resolution of Lilith's suit relating to its source code will not affect their interests.

"Lilith alleges that uCool copied its source code — a series of alphanumeric instructions read by a computer to achieve a particular operation," the judge said. "The proposed intervenors, however, do not claim an interest in Lilith's source code."

Rather, Blizzard and Valve allege Lilith and uCool copied certain visual elements, he said.

While a game's visual elements are generated by source code, he said, copyrighted source code is a "protectable literary work distinct

from and responsible for much more than the generation of visual elements in a game."

Intervention at this stage also would unduly delay resolution of the original parties' case, Judge Conti said.

It would require deliberation of extraneous legal and factual issues the original case would not otherwise invoke, including questions related to the artistic development of characters, settings, terrain, background art and other visual elements, he said.

Judge Conti added that Blizzard and Valve have the option to file a separate lawsuit against Lilith and uCool if they wish to address their own copyright infringement claims. WJ

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

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

Proposed interveners: Daniel Agar Kohler and Karin G. Pagnanelli, Mitchell Silberberg & Knupp, Los Angeles

Related Court Document:
Aug. 17 order: 2015 WL 4914694

See Document Section B (P. 42) for the order.

No duty to defend software provider in copyright-extortion suit

By Thomas Parry, Contributor, Westlaw Daily Briefing

A software company is not entitled to defense or indemnification from its general liability insurer for a licensee's suit alleging the company perpetrated an extortion scheme involving bogus copyright infringement claims, a Boston federal judge has ruled.

PTC Inc. v. Charter Oak Fire Insurance Co., No. 14-cv-14056, 2015 WL 5005796 (D. Mass. Aug. 21, 2015).

U.S. District Judge Douglas P. Woodlock of the District of Massachusetts said Charter Oak Fire Insurance Co. was not required to defend PTC Inc. against the underlying suit because the general liability policy's intellectual property exclusion clearly and unambiguously barred coverage.

ALLEGED EXTORTION SCHEME

In 2013 Flextronics International Ltd., an electronics manufacturer, filed a complaint in the Northern District of California, alleging that PTC, which licensed software to Flextronics, unlawfully accessed and obtained confidential and proprietary information from Flextronics' computers without its consent.

Flextronics' complaint also alleged that PTC had embedded technology into its software to collect proprietary data as part of a scheme to increase revenues by making "knowingly false and/or reckless accusations of copyright infringement and/or unlicensed use of PTC software in [an] effort to extort payments from its customers/licensees."

Flextronics sought a declaration under the Copyright Act, 17 U.S.C. § 106, that it had not infringed PTC's copyrights. It also asserted a claim for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and several claims under California law.

In response, PTC asserted counterclaims, including that Flextronics had infringed PTC's software copyrights.

INTELLECTUAL PROPERTY EXCLUSION

PTC turned to Charter for a defense in the suit under its general liability policy that said Charter would defend PTC in suits seeking damages for personal injury and pay related damages that PTC became legally obligated to pay, according to Judge Woodlock's opinion.

The insurer denied coverage in June 2014 and again September 2014, citing the policy's IP exclusion.

The exclusion barred coverage for personal injury "arising out of any actual or alleged infringement or violation" of copyright law or any other personal injury alleged in a "suit" that also alleges copyright infringement.

> "The counterclaim seems plainly to be within the language of the IP exclusion" the judge wrote.

EXCLUSION APPLIES

In October 2014 PTC sued the insurer in Massachusetts state court seeking a declaratory judgment that Charter was obligated to defend PTC in the underlying Flextronics suit. Charter removed the case to the Massachusetts District Court, and PTC moved for judgment on the pleadings.

The software provider argued that the exclusion did not apply because Flextronics had not alleged copyright infringement against PTC in the underlying complaint.

Judge Woodlock found that while Flextronics' complaint contained no direct claim for copyright infringement against PTC, "paragraphs of allegations related to copyright infringement are woven throughout the Flextronics complaint."

He concluded that, given the exclusion's unambiguously broad language — "arising out of any actual or alleged infringement" — the exclusion extended beyond specific copyright infringement allegations against the insured to include personal injury arising out of a third party's alleged infringement.

In addition, "the connection between the personal injury alleged and the allegation of IP infringement need not be an actual claim for IP infringement, so long as the alleged injury has some causal nexus to an alleged dispute over copyright infringement," the judge wrote.

"Flextronics' allegations about PTC's copyright-related scheme are within the plain language, personal injury 'arising out of alleged infringement,' of the IP exclusion," the judge concluded.

COUNTERCLAIM

The judge also found that PTC's copyright infringement counterclaim might trigger the IP exclusion.

"The counterclaim seems plainly to be within the language of the IP exclusion — it is an allegation of copyright infringement against Flextronics, and it is alleged in the same suit as the Flextronics allegations," Judge Woodlock wrote.

The judge, however, declined to decide whether PTC's counterclaim alone would trigger the IP exclusion as the question was not fully briefed and was "ultimately unnecessary to resolution of this case."

REASONABLE EXPECTATIONS

The judge also rejected PTC's argument that a ruling that the IP exclusion applied via third-party conduct would defeat its reasonable expectations as an insured.

"Having determined above that the language of the IP exclusion clearly and unambiguously covers the allegations in the Flextronics action, PTC's expectations have no further role to play in this analysis," the judge wrote.

Consequently, he denied PTC's motion and directed that judgment be entered for Charter. WJ

Related Court Document:
Opinion: 2015 WL 5005796

Google can't get rights to patents for personalizing searches

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

Google Inc. has failed to convince the top patent appeals court to revive claims that an inventor breached a contract giving the Internet giant rights to technologies for personalizing online searches.

Personalized User Model LLP et al. v. Google Inc., Nos. 14-1841 and 15-1022, 2015 WL 4923205 (Fed. Cir. Aug. 18, 2015).

Breach-of-contract claims against Personalized User Model LLP and inventor Yochai Konig were time-barred, according to the U.S. Court of Appeals for the Federal Circuit, which also refused to review construction of a disputed claim term.

In 1996 Konig entered into an employment agreement with SRI International, a technology research group in Menlo Park, California. The agreement required Konig to disclose any inventions, including software, which he created or discovered during his employment, the opinion said.

While employed at SRI, Konig and a friend not employed by the company generated documents relating to a "personalized information services idea" they called "Personal Web." The documents were marked confidential, according to the opinion.

Konig left SRI in August 1999, two weeks after forming a company called Utopy, where he developed Personal Web products, the opinion said.

The Patent and Trademark Office issued U.S. Patent Nos. 6,981,040 and 7,685,276, both titled "automatic, personalized online information and product services," based on applications Konig filed after he left SRI.

Konig and the patents' co-inventors assigned the rights to the patents' personalized search technology to Personalized User, a Texas-based patent-holding company.

CONCEIVED DURING EMPLOYMENT

In 2009 Personalized User filed suit in the U.S. District Court for the District of Delaware accusing Google of infringing the '040 patent. The '276 patent was added to the litigation in 2010.

REUTERS/Dado Ruvic

After it was revealed during discovery that Konig had "conceived" the technology for the patents while employed at SRI, Google bought "any rights" that SRI might have in the patents for $40,000, according to a motion with the District Court.

In February 2011 Google filed a counterclaim saying Konig's failure to assign the patents to SRI constituted a breach of contract. His employment agreement with SRI required such an assignment unless the inventions were unrelated to Konig's work at SRI or to SRI's business, according to Google.

In the interim, U.S. District Judge Leonard P. Stark construed several claim terms from the patnts. *Personalized User Model LLP v. Google Inc.*, No. 09-525, 2012 WL 295048 (D. Del. Jan. 25, 2012).

In March 2014 a jury determined Google did not infringe the '040 patent or the '276 patent, found all of the asserted claims were invalid and sided with Google on the breach-of-contract claim.

Personalized User moved for judgment as a matter of law on the breach-of-contract claim. Judge Stark granted the motion, saying that Google had not asserted its counterclaim within the applicable three-year statute of limitations. *Personalized User Model LLP v. Google Inc.*, No. 09-525, 2014 WL 1382391 (D. Del. Apr. 7, 2014).

Google appealed the JMOL claim. Personalized User appealed the court's claim construction but did not dispute the infringement or invalidity rulings.

STATUTE OF LIMITATIONS

Google argued that Judge Stark erred in ruling that the limitations period for its counterclaim was not tolled because its injury was "inherently unknowable."

Statutes of limitations in Delaware are tolled for inherently unknowable injuries if the injured party is "blamelessly ignorant."

Personalized User asserted that even if SRI could not have discovered Konig's conception while he was employed there, the company had "sufficient cause to investigate" after he left.

Google failed to show the injury was unknowable or that SRI was blamelessly ignorant, a Federal Circuit panel ruled, siding with Personalized User.

"Considering the competitiveness of companies and institutes in the technical world ... [Konig's] departure and new venture could well have been a 'red flag' that should have generated an inquiry," the panel said.

Google also failed to provide even the "minimum quantum of evidence necessary" to show that SRI's alleged ignorance was blameless, noting that as SRI had various opportunities, including Konig's exit interview, to ask about the inventions' conception.

NO REVIEW OF CLAIM CONSTRUCTION

The panel agreed with Google that it lacked jurisdiction over Personalized User's claim construction appeal.

Because Personalized User did not challenge the jury's verdict of noninfringement on appeal, modifying the claim construction would have no effect on the outcome of the case, the panel wrote.

Thus, the company's appeal of the claim construction did not prevent a live controversy, the panel said.

Personalized User's argument that a change in claim construction might be given preclusive effect in future litigation was of no moment, the panel said, because it "may not provide an advisory opinion on the meaning of a claim term that does not affect the merits of this appeal." WJ

Attorneys:
Plaintiff-cross-appellant (Personalized User): Richard Salgado and Mark C. Nelson, Dentons U.S. LLP, Dallas; Marc S. Friedman, Dentons U.S. LLP, New York

Defendant-appellant: David A. Perlson and Charles K. Verhoeven, Quinn Emanuel Urquhart & Sullivan, San Francisco; Joshua L. Sohn, Quinn Emanuel Urquhart & Sullivan, Washington; Andrea Pallios Roberts, Redwood Shores, Calif.

Related Court Document:
Opinion: 2015 WL 4923205

PATENTS

PTO filings for touch device patents were timely, U.S. and IP owners say

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

The U.S. government and the Intellectual Property Owners Association are backing a Silicon Valley software developer that had three patents deemed invalid because a continuation application was filed on the same day a parent application was granted.

Immersion Corp. v. HTC Corp. et al., No. 15-1574, amicus brief filed (Fed Cir. Aug. 12, 2015).

Amicus briefs supporting Immersion Corp. urge the U.S. Court of Appeals for the Federal Circuit to reverse a lower court determination that the same-day continuation applications were too late, a finding that led to a win for HTC Corp.

Immersion attorney **Joseph R. Palmore**, a partner at **Morrison & Foerster** Washington, said he was pleased that "the United States and industry have urged the Federal Circuit to affirm the law and rules that have been consistently applied for more than 150 years."

Representatives for HTC could not be reached for comment.

In March 2012 Immersion filed a patent infringement suit in the U.S. District Court for the District of Delaware against Taiwanese smartphone maker HTC and its American and British Virgin Island affiliates.

The suit said HTC's MyTouch 4G Slide and other products had infringed several patents covering methods of recognizing information from touch devices on computer screens and smartphones.

In February U.S. District Judge Richard D. Andrews granted partial summary judgment to the defendants. *Immersion Corp. v. HTC Corp. et al.*, No. 12-259, 2015 WL 627425 (D. Del. Feb. 11, 2015).

Immersion appealed after the parties stipulated to dismissal of the remaining claims.

SAME-DAY APPLICATIONS

As part of its defense, HTC had disputed the validity of U.S. Patent Nos. 7,982,720; 8,031,181; and 8,059,105, all of which are titled "haptic feedback for touchpads and other touch controls."

HTC argued that the '720, '181 and '105 patents were invalid as anticipated by a foreign application under Section 102 of the Patent Act, 35 U.S.C. § 102.

The foreign application had a specification identical to the patents' parent and was filed more than one year before applications for the three patents were filed in 2007, the opinion said.

However, the three patents claimed the priority date of their parent, U.S. Patent No. 6,429,846, which was granted on Aug. 6, 2002.

Judge Andrews said Section 120 of the Patent Act, 35 U.S.C. § 120, would give the three patents the priority date of the parent if the three applications were filed before the parent application was granted.

Immersion presented evidence that a continuation application for the three patents was filed on Aug. 6, 2002, the same day the parent application was granted, but it did not present evidence it was filed "before" that day, according to the opinion.

> The government's *amicus* brief disagrees with the District Court's interpretation of the Patent Act, calling the PTO's decades-long practice "reasonable, practical and entitled to deference."

CHEVRON DEFERENCE

Immersion argued that the Patent and Trademark Office has "long given" continuation applications the priority date of a prior application when the continuation is filed on the same day the patent is granted.

As a federal agency, the PTO's practices should be given deference under *Chevron USA Inc. v. Natural Resources Defense Council Inc. et al.*, 467 U.S. 837 (1984), Immersion argued.

Judge Andrews, however, said the PTO was not entitled to *Chevron* deference because the Patent Act is neither "silent" nor "ambiguous" on the issue.

Section 120 "expressly states that the application must be filed 'before' the parent application issues," the judge said.

'FILED BEFORE THE PATENTING'

In its *amicus* brief, the United States disagrees with the District Court's interpretation of the Patent Act, calling the PTO's decades-long practice "reasonable, practical and entitled to deference." *Immersion Corp. v. HTC Corp. et al.*, No. 15-1574, *amicus brief filed* (Fed Cir. Aug. 11, 2015).

The agency's practice of treating same-day continuing applications as filed before the patenting of a parent application "obviates the need to determine the exact second that an application was filed," the brief says.

The PTO's interpretation is faithful to legislative history and "fills a void" left by Congress in the statute, the government says.

The Intellectual Property Owners Association agrees, adding that the PTO's practice is consistent with court interpretations of Section 120 for more than a century, citing *Godfrey v. Eames*, 68 U.S. 317 (1863).

More recently, a Wisconsin federal court deferred to the PTO's practice because of the act's "silence" and the agency's "specialized experience regarding patenting procedure." *MOAEC Inc. v. MusicIP Corp.*, 568 F. Supp. 2d 978 (W.D. Wis. 2008).

For these reasons, the members of the IPOA have come to rely on the PTO's practice, as more than 12,000 patents resulting from continuation applications had filing dates that were the same as their issuing dates, the IPOA's brief says. WJ

Attorneys:
Amicus (IPOA): Philip S. Johnson and Kevin H. Rhodes, Intellectual Property, Owners Association, Washington; George F. Pappas, Paul J. Berman, Ranganath T. Sudarshan and John A. Kelly, Covington & Burling, Washington

Amicus (United States): Acting Solicitor Thomas W. Krause and Associate Solicitors William Lamarca and Farheena Y. Rasheed, U.S. Patent and Trademark Office, Washington

Related Court Documents:
Amicus brief (IPOA): 2015 WL 4995742
Amicus brief (United States): 2015 WL 4995741

NEWS IN BRIEF

SUIT: HP FALSELY ADVERTISES SMART INSTALL PRINTER FEATURE

Hewlett-Packard Co. is facing an amended class-action complaint alleging it falsely markets some of its printers as including HP Smart Install software. Plaintiff Anne Wolf alleges HP advertises that the printers include this feature for quick and easy installation when in fact it has been disabled from the printers sold to her and other consumers. HP's misrepresentations were part of a common scheme to mislead consumers and incentivize them to buy the , in violation of California's false-advertising law, according to Wolf. The suit seeks class certification and an injunction requiring HP to cease misrepresenting the availability of the software. It also seeks full restitution and unspecified punitive damages.

Wolf v. Hewlett-Packard Co., No. 5:15-cv-01221, first amended complaint filed (C.D. Cal. Aug. 17, 2015).

Related Court Document:
First amended complaint: 2015 WL 5093173

HEALTH CARE SOFTWARE MAKER GETS MORE TIME TO ANSWER ANTITRUST SUIT

Health data analytics company OptumInsight Inc. will have until Sept. 16 to answer an antitrust lawsuit alleging it fraudulently procured patents in an attempt to illegally monopolize the market for medical claims organizing software. Cave Consulting Group Inc. alleges OptumInsight unlawfully obtained a portfolio of patents by repeatedly hiding material facts from the U.S. Patent and Trademark Office and affirmatively misstating its prior efforts to commercialize the patented inventions. The company then suppressed competition by threatening to enforce or enforcing its ill-gotten portfolio against competitors in the marketplace, according to the California federal court suit. As a result, OptumInsight's anti-competitive conduct has harmed competition by increasing prices and reducing competition, quality, innovation and consumer choice, the suit says. OptumInsight's answer was due Aug. 17, but the parties agreed in a joint stipulation to extend the deadline 30 days.

Cave Consulting Group Inc. v. OptumInsight Inc., No. 3:15-cv-03424, joint stipulation filed (N.D. Cal. Aug. 14, 2015).

Related Court Document:
Complaint: 2015 WL 4509245

SWEEPSTAKES SOFTWARE MAKER PLEADS GUILTY TO ILLEGAL GAMBLING

Software provider Capital Sweepstakes Systems Inc. and its president have pleaded guilty to conducting an illegal Internet gambling business, the FBI said in a statement. The company and co-defendant Kevin Freels violated California and federal law by misrepresenting their slot-machine-style games as legal "sweepstakes" enterprises, the statement said. As part of the plea agreement, the defendants will forfeit more than $1.5 million in profits generated from the business. The funds were seized by prosecutors in a related proceeding, according to the statement. The defendants also agreed to pay $700,000 in civil penalties to resolve a parallel civil settlement with the California attorney general's office. The defendants are scheduled to be sentenced by U.S. District Judge Morrison C. England Jr. of the Eastern District of California on Nov. 5, the FBI said. Freels faces up to five years in prison and a $250,000 fine.

United States v. Capital Sweepstakes Systems Inc. et al., No. 2:15-cr-00126, plea agreements entered (E.D. Cal. July 30, 2015).

Mutual fund board rightly rejected suit over Internet gaming investment, 8th Circuit finds

The 8th Circuit has affirmed a Missouri federal judge's decision that, under Maryland law, American Century Cos.' directors properly investigated and refused to pursue a shareholder's claims that the mutual fund's board recklessly lost a big bet on an illegal Internet gaming company.

Seidl v. American Century Cos. et al., No. 14-2796, 2015 WL 4978972 (8th Cir. Aug. 21, 2015).

The 8th U.S. Circuit Court of Appeals upheld the ruling that, even though the ACC board's ultimately disastrous approval of a substantial investment in Gibraltar-based PartyGaming Plc. resulted in big losses, it deserved the deference of the business-judgment rule.

The appellate court also affirmed the judge's ruling that a two-director special litigation committee rightly recommended the board not take up shareholder Laura Seidl's proposed breach-of-duty suit over the gaming investment losses. The 8th Circuit found that the business-judgment rule also sheltered the committee's actions.

The business-judgment rule, applied by most state and federal courts nationwide, gives directors' decisions the benefit of the doubt as long as they display independence, objectivity and good faith in making those decisions.

A HOW-TO OPINION

The 8th Circuit's decision likely will be closely examined by corporate law specialists because it provides a step-by-step procedure that has already passed court review for companies responding to derivative shareholder suits.

The appeals court's opinion is especially helpful for litigation committees charged with investigating and making a recommendation on whether a company should take up the charges.

Seidl's suit in the U.S. District Court for the Western District of Missouri said all ACC investors were damaged by the board's decision to have its Ultra Fund invest heavily in a company with websites that facilitated Internet gambling on poker games.

ACC's directors knew there was a good chance U.S. authorities would adopt rules that effectively would prohibit PartyGaming's operations in the United States, where it derived most of its revenue, but declined to pull out or pull back until U.S. regulatory changes spelled party over for PartyGaming, Seidl said.

The fund lost $16 million after it became apparent that PartyGaming would not be operating in the United States.

According to the opinion, in 2010 Seidl demanded that ACC take up her breach-of-duty, negligence and waste charges against the directors who allegedly went out on a limb by having the fund invest in PartyGaming.

The opinion said ACC appointed a committee of two independent directors to investigate Seidl's charges. The committee hired independent counsel, conducted an investigation, reviewed more than 4,000 documents, interviewed dozens of people and issued an 81-page report that recommended the board take no action. The board accepted and approved the report.

Seidl challenged both decisions in federal court, but the judge, applying the corporate law of Maryland, where ACC is incorporated, ruled in the company's favor based on the conclusion that both the committee and the board were protected by the business-judgment rule because of their members' independence, good faith and reasonableness.

On appeal the 8th Circuit said ACC was entitled to summary judgment because it had "come forward with some evidence that the committee conducted a reasonable inquiry upon which its conclusion is based and that no significant business or personal relationships impinged the committee's independence and good faith."

SHIFTING BURDEN

At that point, the burden of proof shifted to Seidl to show the committee lacked independence or objectivity, but she was unable to do so, the appellate panel said.

The 8th Circuit noted the thoroughness of the investigation, the completeness of the 81-page report and the soundness of the recommendation that Seidl's charges were too weak to stand up in court.

The appeals court said that although the committee ultimately excluded a report that ACC's directors continued investing in PartyGaming despite knowing its transactions were illegal that was not proof of bias because it was a preliminary report that was not required to be included in its final recommendation. WJ

Attorneys:
Plaintiff: Thomas I. Sheridan III, Simmons Hanly Conroy LLC, New York

Defendants: William P. Brandt and Nick J. Kurt, Bryan Cave LLP, Kansas City Mo.; Kurt D. Williams, Berkowitz Oliver Williams Shaw & Eisenbrandt, Kansas City, Mo; Steuart H. Thomsen, Sutherland Asbill & Brennan, Washington; Benjamin H. Kleine and Gordon C. Atkinson, Cooley LLP, San Francisco

Related Court Document:
Opinion: 2015 WL 4978972

Online comments

CONTINUED FROM PAGE 1

THE DANZINGER BRIDGE INCIDENT

On Sept. 4, 2005, days after Katrina flooded New Orleans, the police responded to a report of shots being fired at law enforcement near the Danzinger Bridge.

When the responding officers arrived, heavily armed, they shot six unarmed pedestrians, killing one teenager and one developmentally disabled man, and injuring four other civilians.

New Orleans Police Department officers Kenneth Bowen, Robert Gisevius, Robert Faulcon, Anthony Villavaso and Arthur "Archie" Kaufman, and possibly others, allegedly tried to make the shootings appear legally justified.

On July 12, 2010, a grand jury in the U.S. District Court for the Eastern District of Louisiana charged those five officers with civil rights violations, conspiracy and obstruction of justice. Faulcon was also indicted for making a fatal shot.

Other officers, however, took plea deals and cooperated with the prosecution, the majority opinion said.

The five officers who stood trial amid the publicity received prison sentences of between 35 and 65 years. The officers who took plea deals received sentences of between five and eight years.

THE ONLINE COMMENTS

During and after the trial in summer 2011, commenters discussed the bridge events on NOLA.com, which hosts the online version of New Orleans' daily newspaper, The Times-Picayune.

About a year later, the trial court learned Sal Perricone, a high-ranking assistant federal prosecutor in New Orleans, was among those who posted comments anonymously on the site. In his comments about the Danzinger Bridge incident, Perricone berated the defendants and their lawyers and called the city's police department "rotten from the head down," the opinion said.

While Perricone did not represent the government in this case, First Assistant U.S. Attorney Jan Mann did. Mann also served as the chief of the New Orleans office's criminal division and initially she investigated the extent of the office's involvement with the NOLA.com comments for the trial court, the 5th Circuit opinion said.

After assuring the trial judge that Perricone was the "sole culprit," Mann admitted to posting frequent replies to his comments, expressing consistent views, according to the opinion.

A civil rights attorney from the U.S. Department of Justice, Karla Dobinski, also posted anonymously on the website. In her day-to-day duties, however, Dobinski was also responsible for protecting indicted police officers' civil rights, the appellate opinion said.

"That three supervisory-level prosecutors committed misconduct in connection with the Danzinger Bridge prosecution is beyond dispute," Judge Jones said.

Seven out of 12 jurors were aware of the NOLA.com comments, according to the appellate opinion.

"Just as a mob protesting outside the courthouse has the potential to intimidate parties and witnesses, so do streams of adverse online comments," Judge Jones wrote, saying this must have affected the officers' defense strategy.

DISSENTING OPINION

Judge Edward C. Prado dissented from the decision to grant a mistrial, although he did not condone the prosecution's actions.

"Because the majority opinion relies on extraordinary facts to skirt ordinary procedure, I respectfully dissent," he wrote.

Judge Prado focused on the timing of the defendants' motion for a new trial based on newly discovered evidence that at least three anonymous Nola.com commenters came from the U.S. attorney's office in New Orleans.

The jury convicted the defendants Aug. 5, 2011, and they filed an initial motion for a new trial that Aug. 22 after the judge granted an extension. This initial motion, however, did not refer to newly discovered evidence, Judge Prado noted.

More than six months later, in May 2012, the defendants learned about the anonymous commenters' identities and filed a second motion.

"Just as a mob protesting outside the courthouse has the potential to intimidate parties and witnesses, so do streams of adverse online comments," 5th Circuit Judge Edith H. Jones wrote for the majority.

Generally, Rule 33 requires a defendant to file a motion for a new trial within 14 days. Rule 33(b)(1) gives a defendant more time to ask for a new trial based on new evidence, but it requires defendants to meet a strict test: They must show the evidence introduced at a new trial would probably produce an acquittal.

Judge Prado said the appellate majority and the lower court granted the defendants' delayed motion without requiring them to meet the stricter standard, relating it back to the first motion.

"Perhaps this is because the defendants advance no credible argument that the newly discovered evidence in this case — the identity of the commenters on NOLA.com — would likely produce an acquittal," he said. WJ

Attorneys:
Plaintiff-appellant: Elizabeth D. Collery, Barbara Bernstein, Thomas E. Chandler, Jessica Dunsay Silver, Christopher J. Smith and Lisa J. Stark, U.S. Department of Justice, Washington; Assistant U.S. Attorney Kevin G. Boitmann and Assistant U.S. Attorney Theodore R. Carter III, New Orleans

Defendant-appellee: Robin E. Schulberg, Covington, La.; Christopher A. Aberle, Louisiana Appellate Project, Mandeville, La., Lindsay A. Larson III, King, Krebs & Jurgens, New Orleans; Timothy A. Meche, New Orleans; Stephen D. London, New Orleans; William P. Gibbens and Ian L. Atkinson, Schonekas, Evans, McGoey & McEachin, New Orleans

Related Court Document:
Opinion: 2015 WL 4925029

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

CASE AND DOCUMENT INDEX

Bell et al. v. Itawamba County School Board et al., No. 12–60264, 2015 WL 4979135 (5th Cir. Aug. 20, 2015) 7

Cave Consulting Group Inc. v. OptumInsight Inc., No. 3:15-cv-03424, *joint stipulation filed* (N.D. Cal. Aug. 14, 2015) 18

Code Revision Commission et al. v. Public.Resource.org Inc., No. 1:15-cv-02594, *complaint filed* (N.D. Ga., Atlanta Div. July 21, 2015) 8

Doe 1 et al. v. Avid Life Media Inc. et al., No. 8:15-cv-01347, *complaint filed* (C.D. Cal., Santa Ana Aug. 24, 2015) 10

Doe v. Avid Life Media Inc. et al., No. 2:15-cv-06405, *complaint filed* (C.D. Cal., L.A. Aug. 21, 2015) 10

Doe v. Avid Life Media Inc. et al., No. 6:15-cv-01464, *complaint filed* (N.D. Ala. Aug. 25, 2015) 10

Doe v. Avid Life Media Inc., No. 3:15-cv-2750, *complaint filed* (N.D. Tex., Dallas Aug. 21, 2015) 10

Federal Trade Commission v. Wyndham Worldwide Corp., No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) 9

Immersion Corp. v. HTC Corp. et al., No. 15-1574, *amicus brief filed* (Fed Cir. Aug. 12, 2015) 17

In re Adobe Systems Inc. Privacy Litigation, No. 5:13-cv-05226, *motion for approval of voluntary dismissal granted* (N.D. Cal., San Jose Div. Aug. 14, 2015) 12

Khoday et al. v. Symantec Corp. et al., No. 11-0180, *motion for preliminary settlement approval filed* (D. Minn. Aug. 18, 2015) 13

Lilith Games (Shanghai) Co. v. uCool Inc. et al., No. 3:15-cv-01267, 2015 WL 4914694 (N.D. Cal. Aug. 17, 2015) 14
Document Section B 42

PTC Inc. v. Charter Oak Fire Insurance Co., No. 14-cv-14056, 2015 WL 5005796 (D. Mass. Aug. 21, 2015) 15

Personalized User Model LLP et al. v. Google Inc., Nos. 14-1841 and 15-1022, 2015 WL 4923205 (Fed. Cir. Aug. 18, 2015) 16

Seidl v. American Century Cos. et al., No. 14-2796, 2015 WL 4978972 (8th Cir. Aug. 21, 2015) 19

United States v. Bowen et al., No. 13–31078, 2015 WL 4925029 (5th Cir. Aug. 18, 2015) 1
Document Section A 23

United States v. Capital Sweepstakes Systems Inc. et al., No. 2:15-cr-00126, *plea agreements entered* (E.D. Cal. July 30, 2015) 18

Welborn et al. v. Internal Revenue Service et al., No. 1:15-cv-01352, *complaint filed* (D.D.C. Aug. 20, 2015) 11

Wolf v. Hewlett-Packard Co., No. 5:15-cv-01221, *first amended complaint filed* (C.D. Cal. Aug. 17, 2015) 18