

## WHAT'S INSIDE

## PATENT

- 6 Patent exhaustion case added to Supreme Court's queue  
*Impression Products v. Lexmark International* (U.S.)

## COPYRIGHT

- 7 Telecoms back Cox in \$25 million copyright appeal  
*BMG Rights Management v. Cox Communications* (4th Cir.)

## ANTI-SLAPP

- 8 Pot news site can't slap down libel suit, appeals court says  
*Medical Marijuana v. ProjectCBD.com* (Cal. Ct. App.)

## DISCOVERY

- 10 Florida swingers club ordered to give up email list  
*Edmondson v. Velvet Lifestyles* (S.D. Fla.)

## HACKING

- 11 Former baseball player takes third swing at MLB  
*Nix v. Major League Baseball* (N.Y. Sup. Ct.)

## SEARCH &amp; SEIZURE

- 12 Child services official loses appeal over cellphone seizure  
*Reynolds v. State* (Tex. App.)

## TRADE DRESS

- 13 UK resident must fight trade dress suit in California, judge rules  
*Mysfyt Inc. v. Lum* (N.D. Cal.)

## CYBERSQUATTING

- 14 Hacker stole CostaRica.com, suit says  
*CostaRica.com v. <costarica.com>* (E.D. Va.)

## DESIGN PATENT

## Lawyers weigh in on design patent defeat in Apple/Samsung smartphone case

By Melissa J. Sachs

The U.S. Supreme Court has rejected the Federal Circuit's interpretation of the Patent Act for design patent infringement awards, leaving up in the air a \$399 million jury verdict Apple won in a case against Samsung.

***Samsung Electronics Co. et al. v. Apple Inc., No. 15-777, 2016 WL 7078449 (U.S. Dec. 6, 2016).***

The U.S. Court of Appeals for the Federal Circuit should have recognized that design patent damages can be calculated from infringement of just one component of a multicomponent product, such as a smartphone, Justice Sonia Sotomayor wrote for a unanimous court.

Section 289 of the Patent Act, 35 U.S.C.A. § 289, allows design patent owners to collect total profits from an infringing "article of manufacturer," a term the Federal Circuit interpreted to mean only the end product sold to consumers, Justice Sotomayor wrote.

The high court sent the case back to the Federal Circuit to determine the relevant article of manufacture from which to calculate Apple's



REUTERS/Dado Ruvic

damages, opting not to give any further guidance on the issue.

Intellectual property lawyers who were not involved with the case, but who followed it, commented on the decision.

CONTINUED ON PAGE 16

## EXPERT ANALYSIS

## Unshielded: The effects of Brexit on multinational data management

Multinational companies and companies that do business abroad should consider how the U.K.'s exit from the EU — if and when it goes through — may affect data management, says ZL Technologies' Linda Sharp, an information governance, data privacy and security expert.

SEE PAGE 3



## Westlaw Journal Computer & Internet

Published since November 1983

**Director:** Mary Ellen Fox

**Editor:**

Melissa J. Sachs  
Melissa.Sachs@thomsonreuters.com

**Managing Desk Editor:**

Robert W. McSherry

**Desk Editors:**

Alex Horowitz, Jennifer McCreary,  
Katie Pasek, Sydney Pendleton,  
Maggie Tacheny

**Graphic Designers:**

Nancy A. Dubin, Ramona Hunter

**Thomson Reuters**

175 Strafford Avenue, Suite 140  
Wayne, PA 19087  
877-595-0449  
Fax: 800-220-1640  
www.westlaw.com  
Customer service: 800-328-4880  
For more information, or to subscribe,  
please call 800-328-9352 or visit  
west.thomson.com.

For the latest news from Westlaw Journals,  
visit our blog at <http://blog.legalsolutions.thomsonreuters.com/tag/westlaw-journals>.

**Reproduction Authorization**

Authorization to photocopy items for internal or personal use, or the internal or personal use by specific clients, is granted by Thomson Reuters for libraries or other users registered with the Copyright Clearance Center (CCC) for a fee to be paid directly to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923; 978-750-8400; www.copyright.com.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner.



## TABLE OF CONTENTS

<b>Design Patent: <i>Samsung Electronics Co. v. Apple Inc.</i></b> Lawyers weigh in on design patent defeat in Apple/Samsung smartphone case (U.S.) .....	1
<b>Expert Analysis: By Linda G. Sharp, Esq., ZL Technologies</b> Unshielded: The effects of Brexit on multinational data management .....	3
<b>Patent: <i>Impression Products v. Lexmark International</i></b> Patent exhaustion case added to Supreme Court's queue (U.S.) .....	6
<b>Copyright: <i>BMG Rights Management v. Cox Communications</i></b> Telecoms back Cox in \$25 million copyright appeal (4th Cir.) .....	7
<b>Anti-SLAPP: <i>Medical Marijuana v. ProjectCBD.com</i></b> Pot news site can't slap down libel suit, appeals court says (Cal. Ct. App.) .....	8
<b>Discovery: <i>Edmondson v. Velvet Lifestyles</i></b> Florida swingers club ordered to give up email list (S.D. Fla.) .....	10
<b>Hacking: <i>Nix v. Major League Baseball</i></b> Former baseball player takes third swing at MLB (N.Y. Sup. Ct.) .....	11
<b>Search &amp; Seizure: <i>Reynolds v. State</i></b> Child services official loses appeal over cellphone seizure (Tex. App.) .....	12
<b>Trade Dress: <i>Mysfyt Inc. v. Lum</i></b> UK resident must fight trade dress suit in California, judge rules (N.D. Cal.) .....	13
<b>Cybersquatting: <i>CostaRica.com v. &lt;costarica.com&gt;</i></b> Hacker stole CostaRica.com, suit says (E.D. Va.) .....	14
<b>Shareholder Suit: <i>Nagy v. Facebook Inc.</i></b> Facebook's advertising metrics draw shareholder suit (D. Nev.) .....	15
<b>News in Brief</b> .....	17
<b>Case and Document Index</b> .....	18

# Unshielded: The effects of Brexit on multinational data management

By **Linda G. Sharp, Esq.**  
*ZL Technologies*

The U.K.'s forthcoming departure from the European Union has exposed the instability faced by multinational data management initiatives during an era of evolving privacy legislation.

Brexit has regulatory implications for multinational companies with locations in the U.K. and companies that wish to host non-U.K. data in the U.K. In fact, its outcome could send shock waves through the data management space as a whole.

The EU Data Protection Directive requires member countries to adopt legislation that prohibits the transfer of personal data to countries that are not EU members.

## FORMATION OF THE EU

Any insight on the impact of Brexit on multinational data management should be based on an informed understanding of the EU's creation and evolution.

Historian Robert Wilde notes the formation of the EU occurred in several steps and was facilitated by the gradual rise in confidence that each successful step yielded.

After World War II, surrounding nations looked to ensure a collaborative approach to handling economic issues, not just an effort to ensure peace.



European Union flags near Elizabeth Tower in London

REUTERS/Luke MacGregor

They needed a process by which participating countries could exchange goods and services, recognizing that by working together they could rebuild their infrastructures and economies.

This effort was also influenced by their concern to remain independent of the ever-prevalent eastern blockade, which was dominated by the Soviet Union.

Encouraging surrounding nations to join together for a common good would reduce the likelihood of any of them starting another war.

It wasn't until 1973 that the U.K., along with Denmark and Ireland, finally joined.

After years of partnership and collaboration between countries, the EU was officially established in 1993 by the execution of the Maastricht Treaty.

As Bob Dylan once said, "The Times They Are A-Changin'!"

Never in my life did I expect to see the Berlin Wall come down, the split of the Union of Soviet Socialist Republics and now, Brexit.

After much discussion and debate in the U.K. over the viability of an exit from the EU, on June 23, the people of the U.K. spoke loud and clear, voting to leave the EU.

Within days, legal questions began to surface as to whether such an exit required parliamentary approval.

There are processes for EU withdrawal outlined in Article 50 of the Treaty of Lisbon, but this document — only about 250 words long and never tested — is extremely vague.

It is apparent from the treaty's language that its drafters probably never anticipated a withdrawal.

To date, the U.K. has not provided formal notification to the EU of its intent to withdraw.



**Linda G. Sharp** is associate general counsel at **ZL Technologies**, based in Milpitas, CA, and is an expert in the areas of information governance, management and e-discovery. She has spent over three decades in the legal profession and more than 15 years focusing on data management initiatives. Sharp has counseled many federal and state agencies and members of the bench, as well as Fortune 500 entities, on issues concerning e-discovery, information governance, data privacy and security. She can be reached at [lsharp@zlti.com](mailto:lsharp@zlti.com).

From the time that the U.K. invokes the Article 50 provisions, there is a two-year term to work through the process, during which time all 27 remaining EU member states will have to come to a single agreement with the U.K. regarding its exit.

However, this may take longer than the two years anticipated when Article 50 was established.

As The Guardian newspaper reported: "The UK will have to renegotiate 80,000 pages of EU agreements, deciding those to be kept in UK law and those to jettison. British officials have said privately that nobody knows how long this would take, but some ministers say it would clog up parliament for years."

---

## The U.K.'s regulatory position both before and after its exit will affect multinational organizations' handling of data in the country.

---

### EU DATA PRIVACY REGULATIONS

During the 1990s the EU became deeply concerned with the handling of its citizens' personal data.

It developed stringent privacy regulations applicable to all organizations — both within and outside the EU — that host such data.

The EU Data Protection Directive requires member countries to adopt legislation that prohibits the transfer of personal data to countries that are not EU members.

The only exception is for countries that the EU has determined have laws that provide "adequate" protection of personal data.

The U.S. was deemed to not meet this requirement. As such, in Nov. 2000, the U.S.-EU Safe Harbor Program was negotiated by the EU and the U.S. Department of Commerce.

On Oct. 5, 2015, in the matter of Maximilian Schrems versus the Irish Data Protection Commissioner, the European Court of Justice declared the U.S.-EU Safe Harbor agreement invalid.

The agreement controlled and approved transfers between the EU and the U.S. of personally identifiable electronic data of people of the EU.

The ECJ's decision to strike down the agreement left many multinational

companies potentially exposed, having EU data stored in the U.S. and no legitimate regulatory agreement in place.

With surprising speed, the EU adopted the EU-U.S. Privacy Shield to cover such transactions, and certification to receive such data became available on Aug. 1.

Privacy Shield sets restrictions for companies in the U.S. handling EU personal data, as monitored by the U.S. Department of Commerce, and sets forth processes for EU citizens who believe their privacy has been violated.

Organizations must also inform individuals when their information is being collected,

what type of information it is, and how it will be used.

Companies that fail to comply with these regulations will be removed from the list of companies approved for data transfer.

In furtherance of the EU's desire to control access to personal information, the EU General Data Protection Regulation, or GDPR, was entered May 24. However, it is not scheduled to fully take effect until May 25, 2018.

Thus, such regulations may go into effect before the U.K.'s exit is finalized.

Among GDPR's requirements is a mandate that organizations providing services to EU subjects receive consent from subjects before processing their personal data, as well as implement data protection measures.

### BREXIT'S IMPACT

The U.K.'s regulatory position both before and after its exit will affect multinational organizations' handling of data in the country.

EU leaders Martin Schulz, Donald Tusk and Jean-Claude Juncker, together with Dutch Prime Minister Mark Rutte, issued a joint statement June 24, after the British people voted to exit.

"Until this process of negotiations is over, the United Kingdom remains a member of

the European Union, with all the rights and obligations that derive from this. According to the treaties which the United Kingdom has ratified, EU law continues to apply to the full to and in the United Kingdom until it is no longer a member," the joint statement said.

As a result, the U.K. will continue to have the same rights to participate in creating and supporting these regulations.

However, it is unclear whether the U.K. will maintain EU regulations after leaving.

It appears strategically sound to remain compliant, because doing so may allow the U.K. to maintain its current status as an epicenter for EU data housing.

However, the U.K. is leaving in large part to avoid EU regulations, so in that sense, it would be counterproductive.

Whichever path the U.K. takes, to continue as a viable local for storage of EU data, U.K. companies will have to adapt to the GDPR by 2018. However not knowing which regulations they will have to meet directly following the exit leaves data management initiatives in limbo.

With the U.K.'s exit from the EU, and the overwhelming number of multinational organizations that either host their EU data in the U.K. or have their EU operations headquartered in the U.K., it is currently unclear exactly how the exit will affect the country and its strategic position for hosting data.

In addition to being a strategic location for headquartering EU operations of non-EU organizations, the U.K. has been a pivotal locale for hosting data for cloud-based providers. Its status in this regard is now unclear.

We have recently started to see other EU nations such as Ireland emerge as attractive destinations for EU operations of U.S. companies, with the likes of Facebook and Microsoft opening local offices.

A KPMG white paper titled "The Brexit Strategy: The Impact on Brexit on US Companies with UK Holdings," observes on page two, "Traditionally, the U.K. has been one of the most attractive destinations in the EU for non-EU companies for establishing a European holding company."

The paper further states: "Multinationals with a U.K.-based holding company

structure should evaluate whether their current structure makes sense in the post-Brexit world. Relocation of the European headquarters to an EU member state may result in a more efficient organization of their business.”

The white paper continues to say that Germany may be an attractive option for relocation, thanks to its tax benefits, “productive labor force,” and “diverse economy.”

Whether it is Germany or another country that rises to fill this void, it is apparent that the U.K. cannot afford a misstep through this process or it will risk its current premier status.

It is possible that the EU will pressure the U.K. into agreeing to follow the Privacy Shield terms if it wishes to continue trade with the EU. If that happens, the U.K. may face the challenge of conducting its own logistical exit from the EU at the same time it is trying to implement adequate technology infrastructure to support the Privacy Shield.

However, because the Privacy Shield, as currently written, requires that businesses dispose of personal data that is no longer needed for active business use, if the U.K. decides not to follow the EU standards for data transfer, it will likely face a large technological challenge in separating U.K. citizen data from EU citizen data and implementing appropriate life cycle and retention policies.

Alternatively, the U.K. could participate in the following agreements with the EU, in which case it would have to negotiate to ensure its eligibility to receive EU personally identifiable data:

- European Economic Area: This allows in part for participation in the EU internal market and ease of movement of goods, services, people and capital. Norway has taken advantage of this format.
- European Free Trade Association: This allows for participation in

intergovernmental organization promoting free trade and the U.K. may negotiate a bilateral trade agreement with the EU. Switzerland currently has such an agreement in place.

- Independent agreements under the World Trade Organization: These agreements are open to negotiation and are not part of any customs free trade opportunities.

We live in a virtual world, and transfer of data between multiple countries is commonplace. Data has no true nationality, yet it must be treated as if it does for purposes of EU regulations, complicating the transfer of data from the EU.

---

### It is unclear whether the U.K. will maintain EU regulations after leaving.

---

Once its exit is complete, the U.K. will have to make regulatory decisions that may affect its ability to continue as an approved country for managing EU data and, as such, EU data for e-discovery purposes.

Companies that have a cross border presence between the EU and the U.K. may face significant issues if the U.K. fails to adopt the EU’s current regulations for handling of its data.

Differences in personal data retention regulations could cause a discrepancy in data retention for companies with both U.K. and EU divisions, which may result in litigants seeking the U.K. version of documents where possible.

These regulations could also impact venue shopping. When the opportunity presents itself, U.S. companies that must litigate in Europe may wish to strategically determine if the U.K. is a more favorable venue based on its privacy requirements as compared with its EU counterpart.

In any event, the decisions that the U.K. now faces regarding its continued relationship with the EU, specifically with regard to managing EU data, could have catastrophic financial consequences.

### HURRY UP AND WAIT

The future impact of the Brexit decision is not clear, especially for corporate technology and information governance initiatives.

It would not be surprising to see a general slowdown of enterprise information technology purchases in the immediate future, as organizations take time to strategize and regroup.

Large technology purchases will likely be stalled, unless the technology in question is completely unrelated to any changes that might happen under Brexit.

As the U.K.’s next steps become clear, multinational organizations and those with data currently stored in the U.K. would be wise to assemble dedicated committees to monitor the overall process and its effects on their organization.

Such a committee should include key stakeholders across diverse roles, including but not limited to legal, risk and compliance, IT, finance, records management, and even positions that regularly handle personal data, such as marketing and human resources.

The success of U.K. and multinational companies in meeting requirements for Brexit — and possibly the Privacy Shield and GDPR — will likely be determined by the strength of their existing information governance policies and practices.

Implementing processes today to identify which data may be affected, reducing those data stores by eliminating information that is no longer viable to the organization, and implementing a forward-looking strategy may result in a much smoother transition as the Brexit process materializes over the next few years. **WJ**

## Patent exhaustion case added to Supreme Court's queue

By Patrick H.J. Hughes

Printer cartridge reseller Impression Products has convinced the U.S. Supreme Court to hear arguments over the applicability of the patent exhaustion doctrine, hoping the high court will overturn a Federal Circuit win for printer manufacturer Lexmark International.

***Impression Products Inc. v. Lexmark International Inc., No. 15-1189, 2016 WL 1117396, cert. granted (U.S. Dec. 2, 2016).***

The high court agreed to consider whether patent exhaustion applies in foreign jurisdictions, a decision that could have significant consequences for various industries engaged in international trade.

Generally, the patent exhaustion doctrine terminates the right to sue a customer who purchased an authorized patented product, meaning patent holders cannot prohibit resales or set a resale price.

However, in the case involving Impression and Lexmark, the full U.S. Court of Appeals for the Federal Circuit ruled that the doctrine does not apply to products first sold abroad or sold with certain post-sale restrictions.

Impression wants the Supreme Court to declare that a sale abroad exhausts a U.S. patent holder's right to sue for infringement, as the court recently held in a decision over copyrighted works.

"Once again the Supreme Court has granted cert. in a case where the Federal Circuit drew



"Once again the Supreme Court has granted cert. in a case where the Federal Circuit drew a distinction between patent and copyright law""  
Kirkland & Ellis partner John C. O'Quinn said.

a distinction between patent and copyright law," said Kirkland & Ellis partner John C. O'Quinn, who is not involved in the case.

"The Supreme Court's decision to review the case shows that at least some on that court believe as a presumptive matter that where they address similar issues, patent and copyright law should be interpreted to reach the same result," O'Quinn added.

### PATENT EXHAUSTION

The case concerns discounted single-use cartridges Lexmark sold under a program that expressly prohibited resale and required buyers to return empty cartridges for recycling.

Impression obtained Lexmark's cartridges in the U.S. and abroad, modified them to circumvent the patented single-use design, and resold them in the U.S., according to court documents.

When Lexmark sued for infringement, Impression presented a first-sale defense, arguing that Lexmark could not enforce patent rights after the first sale.

The case eventually made it to the Federal Circuit.

In a 10-2 decision in February, the en banc court said Lexmark's foreign sales did not exhaust the company's right to sue for patent infringement in the U.S. *Lexmark Int'l v. Impression Prods.*, 816 F.3d 721 (Fed. Cir. 2016).

Regarding the post-sale restrictions, the Federal Circuit reiterated its decision in *Mallinckrodt Inc. v. Medipart Inc.*, 976 F.2d 700 (Fed. Cir. 1992), that a "single-use only" restriction was a valid condition for the resale of a patented medical device and did not prevent a patent owner from suing for infringement.

In March, Impression asked the high court to review the Federal Circuit's ruling.



### FOLLOWING KIRTSAENG

In its petition Impression noted the Supreme Court recently eliminated boundaries for the first-sale doctrine for copyright holders in *Kirtsaeng v. John Wiley & Sons Inc.*, 133 S. Ct. 1351 (2013).

The *Kirtsaeng* court said foreign and domestic sales alike exhaust a copyright holder's right to sue for infringement in the United States. Impression says the same logic should apply to patent cases.

The company also says the Federal Circuit's decision erroneously removed important limits on patent rights, adding that "there is no room in the exhaustion doctrine for continuing post-sale restrictions."

Numerous friend-of-the-court briefs, submitted by such amici as Public Knowledge and the Electronic Frontier Foundation, supported Impression's arguments, urging the high court to reverse the Federal Circuit's decision.

Lexmark, on the other hand, said precedent has already answered the questions Impression raised.

"Because patent law precedents offer no conflict or other reason to grant review, Impression looks to this court's interpretation of the Copyright Act in *Kirtsaeng*," Lexmark's opposition brief said.

## U.S. GOVERNMENT'S ADVICE

The government chimed in with its opinions about the case in October.

"This court has repeatedly found patent rights exhausted ... even when the patentee attempted to impose restrictions on post-sale use or resale," the government's brief said.

The government also said the high court should review the Federal Circuit's proclamation that foreign sales never trigger the exhaustion of U.S. patent rights.

The U.S. government advocated a rule of "presumptive exhaustion," whereby patent owners can reserve their domestic patent rights after authorized foreign sales through an express license, but those rights otherwise expire automatically.

This understanding follows legislation enacted by Congress and free trade agreements signed by the president, the government said. [WJ](#)

## Attorneys:

*Petitioner:* Edward O'Connor, Avyno Law, Encino, CA; Andrew J. Pincus, Paul W. Hughes and Matthew A. Waring, Mayer Brown LLP, Washington, DC

*Respondent:* Timothy C. Meece, V. Bryan Medlock Jr., Jason S. Shull and Audra C. Eldem Heinze, Banner & Witcoff, Chicago, IL; Steven B. Loy, Stoll Keenon Ogden PLLC, Lexington, KY; Constantine L. Trela Jr. and Robert N. Hochman, Sidley Austin LLP, Chicago, IL; D. Brent Lambert, Lexmark International Inc., Lexington, KY

## Related Filings:

Amicus brief (U.S.): 2016 WL 5957534  
Reply brief: 2016 WL 3098606  
Opposition brief: 2016 WL 2997339  
Certiorari petition: 2016 WL 1130030

---

## COPYRIGHT

# Telecoms back Cox in \$25 million copyright appeal

By Nana Ama Sarfo

The American Cable Association and several internet service providers say a federal appeals court should overturn a \$25 million verdict imposed on Cox Communications Inc. for contributory copyright infringement arising from its internet subscribers' alleged piracy activities.

### **BMG Rights Management (US) LLC v. Cox Communications Inc. et al., No. 16-1972, brief filed (4th Cir. Nov. 14, 2016).**

The ACA — along with trade groups that represent the U.S.' largest telecommunications companies — have filed amicus briefs urging the 4th U.S. Circuit Court of Appeals to reverse a district court decision that denied Cox "safe harbor" status and immunity from its subscribers' alleged piracy under the Digital Millennium Copyright Act.

If the decision and verdict from the U.S. District Court for the Eastern District of Virginia are allowed to stand, ISPs will face increased liability just by doing their normal business and will have to restrict or terminate internet access to customers who are merely accused of copyright infringement, the organizations say in their respective briefs.

## UNDERLYING BATTLE

Music company BMG sued Cox in November 2014 alleging over 200,000 Cox subscriber accounts repeatedly infringed its musical works between 2012 and 2014, in violation of the federal DMCA, 17 U.S.C.A. § 512. *BMG Rights Mgmt. (US) LLC v. Cox Enters. Inc.*, No. 14-cv-1611, *complaint filed* (E.D. Va. Nov. 26, 2014).

BMG said the works were illegally downloaded and exchanged through BitTorrent, a peer-to-peer file-sharing protocol.

BMG learned of the alleged infringement from Rightscorp Inc., a copyright enforcement company that BMG hired to monitor BitTorrent sites for illegal content exchanges, according to the complaint.

When Rightscorp believes infringement has occurred through a particular IP address, it sends an infringement notice to the ISP that assigned the address and asks it to forward the notice to its subscriber.

Rightscorp's notices contain a "settlement solution" that allows alleged infringers to pay to avoid litigation, according to Cox's brief before the 4th Circuit. The notices also warn that those who fail to settle could be liable for up to \$150,000 per infringement and could also have their ISP service suspended.

## RIGHTSCORP BLOCKED

Rightscorp sent Cox roughly 1.8 million notices on BMG's behalf, but the ISP never received the notices and therefore did not forward them to its customers, according to the appellate brief.

Cox had previously "blacklisted" Rightscorp for harassing the company and inundating its

system with as many as 24,000 notices in a day. As a result, Cox auto-deleted every email from Rightscorp, including the BMG emails, without reading them.

After BMG sued Cox, a jury found the ISP liable for contributory infringement and awarded the music company \$25 million in damages. The District Court upheld the verdict in August.

Cox then appealed to the 4th Circuit, saying the District Court decision "eviscerates" the DMCA safe harbor for internet service providers.

## AMICI BRIEFS

The ACA says the 4th Circuit must restore integrity to the DMCA by reversing the lower court decision. Otherwise, ISPs will have to treat every notice as proof of actual infringement and will have to terminate service for a large number of subscribers who may not have actually infringed.

Alternately, ISPs will have to investigate every single claim, the plaintiff says.

"This creates troubling precedent regarding how ISPs must react when receiving millions of notices of alleged P2P infringement from an entity (Rightscorp) that has a financial

interest in distributing as many notices as possible," the brief says.

In a separate brief, the United States Telecom Association, which represents telecommunications providers, says the lower court failed to fully understand the implications of its decision. USTelecom says copyright holders are threatening ISPs more aggressively in the wake of the District Court's order.

"The court's order impedes federal telecommunications policy designed to increase internet access because it compels ISPs to restrict internet access based on untested allegations of infringement to qualify for DMCA safe harbor protection," USTelecom said.

The Internet Commerce Coalition, which counts Google, Amazon and Comcast among its members, filed a brief saying the lower

court decision could unbalance the statutory compromise that Congress created between copyright owners and ISPs when it enacted the safe harbor provision of the DMCA. **WJ**

#### Related Filings:

Amicus brief (ACA): 2016 WL 6777625

Amicus brief (USTelecom): 2016 WL 6777624

Amicus brief (Internet Commerce Coalition):

2016 WL 6777626

Opening brief: 2016 WL 6646404

Verdict form: 2015 WL 10844471

District Court complaint: 2014 WL 11030947

## ANTI-SLAPP

# Pot news site can't slap down libel suit, appeals court says

By Melissa J. Sachs

A news website that publishes medical marijuana research cannot dodge a \$100 million libel lawsuit using a California statute that protects free speech, but it may be able to win dismissal on other grounds, a state appeals court has ruled.

***Medical Marijuana Inc. et al. v. ProjectCBD.com et al.*, No. D068523, 2016 WL 6835522 (Cal. Ct. App., 4th Dist., Div. 1 Nov. 21, 2016).**

California's anti-SLAPP law, Cal. Civ. Proc. Code § 425.16, protects defendants named in "strategic lawsuits against public participation," or suits meant to intimidate critics who are commenting on issues of public interest or importance to keep them from engaging in free speech.

Medical Marijuana Inc.'s libel and false-light claims against ProjectCBD.com did not implicate the cannabis research website's protected speech, so the anti-SLAPP law could not be used as a defense to the lawsuit, the 4th District Court of Appeal said.

MMI alleged other defendants, not ProjectCBD, posted defamatory statements about an MMI subsidiary on Facebook, according to the three-judge panel.

The appeals court remanded the case, saying its opinion did not prevent ProjectCBD from seeking to dismiss those claims on other grounds.

### 'HEMP OIL HUSTLERS'

According to the opinion, MMI filed the libel lawsuit along with its subsidiary HempMeds PX LLC against ProjectCBD and seven other defendants, including Jason Cranford and his Colorado medical marijuana dispensary, Rifle Mountain LLC.



REUTERS/Mario Anzuoni/File Photo

***Medical Marijuana Inc. alleged some of the defendants posted defamatory statements about an MMI subsidiary on Facebook, the opinion said. Medical marijuana is shown here.***

HempMeds, which is located in Poway, California, manufactures Real Scientific Hemp Oil, a product containing cannabidiol, or CBD, from the cannabis plant, the opinion said.

Cranford's Rifle Mountain competes with HempMeds and also sells CBD products, the panel said.

According to MMI and HempMeds, in 2014, Cranford posted various negative statements on Facebook about HempMeds' Real

Scientific Hemp Oil product the year before, the opinion said.

In April 2014 he announced his intention to lab-test RSHO for contaminants after he heard about adverse health reactions, the panel said.

He also requested that people contact him if they had negative reactions to RSHO, according to the opinion.

In June 2014 Cranford republished a comment from a mother who allegedly

claimed her daughter is dead because of RSHO, the opinion said.

That October, ProjectCBD posted an article on its website, titled "Hemp Oil Hustlers," about MMI, HempMeds and RSHO, according to the opinion.

The article claimed to have evidence that RSHO was contaminated with heavy metals and solvents. It also alleged multiple people became ill after using RSHO, the opinion said.

MMI and HempMeds sued Cranford, ProjectCBD, the article's author and others in the San Diego County Superior Court, saying MMI's stock plummeted after these false publications.

The suit included counts for libel, trade libel, false light, negligence and intentional infliction of emotional distress.

### ANTI-SLAPP AND A DEFENDANT'S SPEECH

ProjectCBD responded that California's anti-SLAPP law protected it from the suit.

Judge Joel R. Wohlfeil granted ProjectCBD's motion on the claims of trade libel, negligence and emotional distress, but allowed the libel and false-light claims to continue.

While the anti-SLAPP law protects a defendant's free speech rights, it does not shield the defendant from legitimate defamation actions. So, to defeat an anti-SLAPP motion, a plaintiff must show a probability of prevailing on the defamation claim, Judge Wohlfeil explained.

He found MMI and HempMeds sufficiently claimed ProjectCBD published false statements and failed to correctly cite sources, which supported a finding that the website's actions constituted an extreme departure from reasonable publishing standards.

ProjectCBD appealed the ruling.

The Court of Appeal agreed with Judge Wohlfeil that the anti-SLAPP law did not protect ProjectCBD, but it departed from his reasoning.

Regarding the libel and false-light allegations, the relevant complaint, filed Jan. 16, 2015, only referenced the Facebook posts from April until June 2014 made by other defendants. It did not implicate ProjectCBD's speech or publishing activities, the panel said.

The panel said it would not redraft the libel and false-light allegations specified in the complaint to include claims directed against ProjectCBD so that it could then decide whether the claims survive an anti-SLAPP motion. **WJ**

#### Attorneys:

*Appellants:* Tyler R. Andrews, Greenberg Traurig LLP, Irvine, CA

*Respondents:* Kendra J. Hall, Procopio Cory Hargreaves & Savitch, San Diego, CA; Phillip E. Koehnke, Encinitas, CA

#### Related Filing:

Opinion: 2016 WL 6835522

**See Document Section B (P. 28) for the opinion.**

## The WESTLAW JOURNALS blog is your source for the latest developments

in practice areas like business and finance, IP and technology, product liability, and environmental law.

Daily postings from our attorney-editors keep you up to date on important news and analysis and provide a look at what they're working on for future print issues of Westlaw Journals.



To access the blog, visit <http://blog.legalsolutions.thomsonreuters.com/tag/westlaw-journals>

## Florida swingers club ordered to give up email list

By Melissa J. Sachs

A private swingers club “for men and women who enjoy nudity and sexual activity” must disclose its email distribution list in a case alleging it misappropriated photos of a former Playboy Playmate and others in advertisements, a federal judge has ruled.

**Edmondson et al. v. Velvet Lifestyles LLC et al., No. 15-cv-24442, 2016 WL 7048363 (S.D. Fla. Dec. 5, 2016).**

Velvet Lifestyles LLC could not convince U.S. Magistrate Judge Jonathan Goodman of the Southern District of Florida that its email distribution list was a confidential trade secret or was protected by the First Amendment’s associational privilege.

The judge ordered the swingers club, which does business as Miami Velvet, to disclose the list to Jaime Faith Edmondson, a former Playboy Playmate and former Miami Dolphins cheerleader, and the other 31 professional models listed as plaintiffs in the false advertising case.

Miami Velvet is a private adult lifestyle nightclub housed in a 20,000-square-foot building that “gives you the freedom to express yourself in your sexiest attitude and attire,” according to its website.

Edmondson and the other professional models say the swingers club used their photos without authorization on miamivelvet.com and social media outlets to advertise events and for other commercial purposes.

In an amended complaint filed Sept. 15, the models say the swingers club placed the unauthorized images next to more explicit and hardcore pornographic photos, harming their professional reputations.

“Such explicit, hardcore images purport to reflect sex acts performed at the club by club patrons and at all times the intent was to intimate that plaintiffs also participated in such activities,” the amended complaint says.

The suit alleges the swingers club violated the false-advertising and false-endorsement provisions of the Lanham Act, both subdivisions of 15 U.S.C.A. § 1125(a).

It asks for more than \$22 million.

To prove the false-advertising claim, Edmondson and the other models seek to have an expert conduct a customer confusion survey, according to Judge Goodman’s order.

The expert proposes to invite recipients on Miami Velvet’s email list to answer questions similar to those he asked in a separate case against Caliente Resorts and Caliente Vacation Club, a swingers resort and time-share-style club, the order said, citing *Edmondson et al. v. Caliente Resorts LLC et al.*, No. 15-cv-2762.

The *Caliente* case involves some of the same model plaintiffs and raises similar Lanham Act issues.

In that case, the expert used the survey responses to prepare a report concluding that Caliente’s members believed the models agreed to promote the resort and personally represent the associated lifestyle, Judge Goodman said.

Without ruling on whether the expert’s report would be admissible in this case, Judge Goodman said the models may obtain Miami Velvet’s email list to conduct a similar survey.

He rejected the club’s argument that the email list was a trade secret that had independent economic value.

The judge also said the swingers club never showed how disclosing its email distribution list under a protective order would violate an associational privilege, if one even exists.

To reach this conclusion he distinguished the email list, which was compiled for advertising and marketing purposes, with the club’s membership list.

“The profit-oriented, ‘clothing optional’ swingers parties that Miami Velvet’s members attend are social events, and defendants have not established that they are the kind of expressive association protected by the First Amendment,” the judge said.

Additionally, the models showed they need the marketing-email list to conduct market research, while the club failed to demonstrate the recipients would be harassed or face reprisals if the list were disclosed under a court order, the judge said. **WJ**

**Attorneys:**

*Plaintiffs:* Christopher G. Oprison, Akerman LLP, Washington, DC; Naim S. Surgeon, Ackerman LLP, Miami, FL

*Defendant:* Luke Charles Lirot, Clearwater, FL

**Related Filing:**

Order: 2016 WL 7048363

**See Document Section C (P. 38) for the order.**

## Former baseball player takes third swing at MLB

By Daniel E. Ostrach

An ex-professional baseball player turned “sports science guru” has filed his third suit alleging Major League Baseball ruined his training and sports medicine business by connecting his company to a steroids scandal, then hacking and disabling his online accounts.

***Nix et al. v. Major League Baseball et al., No. 159953/2016, complaint filed (N.Y. Sup. Ct., N.Y. Cty. Nov. 28, 2016).***

Florida resident Neiman Nix filed a complaint in the New York Supreme Court, New York County, seeking damages for MLB’s “outrageous, wanton, willful and malicious” conduct and a permanent injunction prohibiting MLB from further destroying his business.

### AN 0-2 COUNT

After Nix suffered a career-ending injury, in 2012 he started DNA Sports Performance Lab Inc., a sports science testing facility in Miami Beach, Florida, according to his complaint.

DNA Sports Lab develops and sells “bio-identicals/nutraceuticals” supplements custom designed for individual clients and which may contain a natural, nonsynthetic insulinlike growth factor, or IGF-1, as a primary ingredient, the complaint says.

Nix says DNA Sports Labs’ line of products is approved by the World Anti-Doping Agency and is “bioidentical to IGF-1.”

The WADA lists IGF-1 “and its analogues” on its list of prohibited substances.

After a scandal involving professional baseball players and a South Florida clinic known as Biogenesis surfaced in 2013, Nix says MLB hired investigators to investigate other Florida clinics, including DNA Sports Lab.

As part of the investigation, Nix says MLB told DNA Sports Lab clients and potential customers it was marketing and selling prohibited substances.

In response, Nix sued MLB and its investigators in Florida state court in 2014. That complaint was dismissed Nov. 6, 2014.

According to the current suit, MLB retaliated against Nix for filing the Florida complaint by hacking and attacking DNA Sports Lab’s social media accounts, hacking and destroying his former attorney’s computer, and eventually disabling his PayPal account.

As a result Nix and DNA Sports Lab have lost millions of dollars in sales, the complaint says.

Nix says he learned from a computer expert the attacks were connected to IP addresses belonging to MLB in New York and Florida.

Nix again sued MLB, its officers and employees, this time in New York federal court, July 14, 2016.

According to Nix, MLB responded by falsely claiming that he “admits to selling products purportedly containing at least one banned performance-enhancing substance (IGF-1).”

Nix voluntarily dismissed his New York federal complaint against MLB on Nov. 3. *Nix et al v. Major League Baseball et al., No. 16-cv-5604, notice of voluntary dismissal* (S.D.N.Y. Nov. 3, 2016).

Nix then filed this complaint in New York state court, alleging MLB tortiously interfered with his business relationships by linking him to the Biogenesis scandal and by hacking into and disabling his online accounts.

The complaint also alleges MLB’s statement in response to his federal lawsuit defamed him by falsely implying he sells banned performance-enhancing substances.

Finally, the complaint alleges MLB violated the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030, by hacking and disabling his online accounts.

Nix seeks monetary damages and a permanent injunction against MLB, its officers and employees preventing them from further destroying his business. [WJ](#)

**Attorney:**

*Plaintiff:* Vincent P. White, New York, NY

**Related Filing:**

Complaint: 2016 WL 7014072

## Child services official loses appeal over cellphone seizure

By Susan Newman

A former supervisor with Texas' child protection services agency has failed to convince a state appeals court to overturn a jury verdict finding her liable for seizing and searching a detained juvenile's cellphone.

**Reynolds v. State, No. 06-15-194, 2016 WL 6995033 (Tex. App., Texarkana Nov. 30, 2016).**

The juvenile runaway had a reasonable expectation of privacy that was breached by the official's warrantless search of the phone, the Court of Appeals in Texarkana said.

The trial court was reasonable in finding that by taking the cellphone and searching it, Natalie A. Reynolds abused her authority as a supervisory employee of the Texas Department of Family and Protective Services, the three-judge panel said.

The panel also said the state provided sufficient evidence that Reynolds knew her actions were unlawful, making her guilty of official oppression, an abuse-of-authority violation that can result in jail time.

### SEARCH AND SEIZURE

In June 2012 Texas police officers sent a 15-year-old girl to a juvenile detention center after she ran away from home, according to the panel's opinion.

While the girl, referred to as A.K. in court documents, was detained, the center confiscated her jewelry and cellphone, the opinion said.

Reynolds, who may have been working with a department investigator, said she took the phone and searched it for contact information related to drug dealers, according to the opinion. She then asked A.K. about two men whose contact information appeared in the phone, the opinion said.

The department did not have court-ordered temporary custody of A.K. until a day after Reynolds searched the phone, the opinion said.

### CHARGES FILED

In 2013 the state charged Reynolds with official oppression arising from her search and seizure of A.K.'s phone.

To convict Reynolds of official oppression under Section 39.03(a)(1) of the Texas Penal Code, Tex. Penal Code Ann. § 39.03(a)(1), the state was required to prove that she intentionally subjected A.K. to an unlawful search or seizure, the opinion said.

The state also was required to prove that Reynolds knew her actions were unlawful at the time, the opinion said.

A jury found Reynolds guilty, and she appealed, challenging the legal sufficiency of the evidence supporting her conviction.

### EVIDENCE OF INTENT

The panel found sufficient evidence, including testimony from Reynolds' former co-workers, to show Reynolds, either by herself or with others from her department, intentionally seized and searched the phone without A.K.'s permission.

The panel rejected Reynolds' claim that her actions fell within the department's guidelines and were therefore lawful.

Reynolds also could not benefit from a Texas law that allows parents to seize their child's property in emergency situations, as the panel pointed out Reynolds was not acting as A.K.'s de facto parent.

Rather, the panel agreed with the state that Reynolds was acting as an investigator in an attempt to build a case for law enforcement and retained the phone to find "drug evidence."

Under the circumstances, A.K. had a reasonable expectation of privacy under the Fourth Amendment during her temporary detention, the panel said.

Reynolds' actions were not authorized because she did not seize the phone in connection with an arrest or pursuant to a warrant, the panel reasoned.

### COURT: SUPERVISOR KNEW HER ACTIONS WERE UNLAWFUL

There was also sufficient evidence that Reynolds knew her actions were criminal or tortious, the panel said.

While Reynolds claimed she reasonably believed her actions were legal, the panel said she should have known better.

"There is evidence that all department investigators are required to attend several days of training on the Fourth Amendment and that Reynolds completed such training well before the date of the incident at issue," the panel said.

Although the panel admitted privacy rights are not easy to understand, several other department employees said they had believed Reynolds' actions were unlawful and expressed concerns to her.

"If Reynolds' subordinates knew her actions were unlawful, Reynolds knew her actions were unlawful as well," the panel concluded.

**WJ**

#### Attorneys:

*Appellant:* M. Michael Mowla, Cedar Hill, TX

*Appellee:* Steven Lilley and Noble D Walker Jr., Hunt County District Attorneys Office, Greenville, TX

#### Related Filing:

Opinion: 2016 WL 6995033

# UK resident must fight trade dress suit in California, judge rules

By Melissa J. Sachs

A U.K. resident who sold 20 percent of his skin care products to California residents through Amazon.com must defend against a San Francisco-based competitor's trade dress infringement suit in a U.S. federal court, a magistrate judge has ruled.

## ***Mysfyt Inc. v. Lum, No. 16-cv-3813, 2016 WL 6962954 (N.D. Cal., Oakland, Nov. 29, 2016).***

U.S. Magistrate Judge Kandis A. Westmore of the Northern District of California rejected foreign defendant James Lum's argument that he lacked the requisite minimum contacts with the state to have to defend against Mysfyt Inc.'s infringement suit.

She said he should have foreseen his actions would harm Mysfyt, a California company, and haling him into the state to defend against the infringement suit was reasonable.

## **SAME PACKAGING AND INSTRUCTIONS, ACNE.ORG SAYS**

According to the judge's order, San Francisco-based Mysfyt owns Acne.org, an online community of more than 500,000 members and 2.5 million monthly visitors.

The website offers information and advice to fight acne, including the Acne.org Regimen, a proprietary, online, step-by-step guide on how to use the company's treatment products.

The guide describes using the Acne.org Treatment, a proprietary, gel-based 2.5 percent benzoyl peroxide product that Mysfyt sells through its website and Amazon.com, the order said.

In July Mysfyt sued Lum, a U.K. resident, who does business as Claror Skin Care.

According to the complaint, since about 2014 Claror Skin Care has sold competing acne and skin care products, mainly through Amazon.

The products include a 2.5 percent benzoyl peroxide gel with packaging designed to confuse consumers, the suit says.

Since 2003 Mysfyt has sold this product in a white, 8-ounce plastic tube with a distinctive red or orange stripe on the side, according to the complaint.

Claror Skin Care's product, which copies Mysfyt's unique gel formula, is packaged in the same 8-ounce plastic tube with the same colored-stripe design and font as Mysfyt's product, the complaint alleges.

The instructions on Claror Skin Care's product direct customers to apply "one

finger's length of the product" to the face — identical to language that Mysfyt uses on its products, the suit says.

The suit accuses Lum of federal trademark infringement, unfair competition and false designation of origin in violation of the Lanham Act, 15 U.S.C.A. § 1125, and unfair competition in violation of California law, Cal. Bus. & Prof. Code § 17200.

## **JURISDICTION REASONABLE**

Lum filed a motion to dismiss the action, contending the court lacked personal jurisdiction over him.

Judge Westmore disagreed.

She found the court had specific personal jurisdiction because Lum sold the allegedly infringing products to California customers, even if these transactions only constituted 20 percent of his total sales.

Lum also sponsored his products on Amazon so customers would see them in search results if they typed in competitors' names, including Acne.org, the judge said.

The defendant should have foreseen his actions would affect San Francisco-based Mysfyt, the order said.

The judge also found jurisdiction would be reasonable over the foreign defendant because Lum used a Florida-based manufacturer and sold most of the allegedly infringing products in California.

"Defendant cannot do business in the United States, [allegedly] infringe on the rights of a United States corporation and not expect to be hauled into court in the United States," Judge Westmore wrote. [WJ](#)

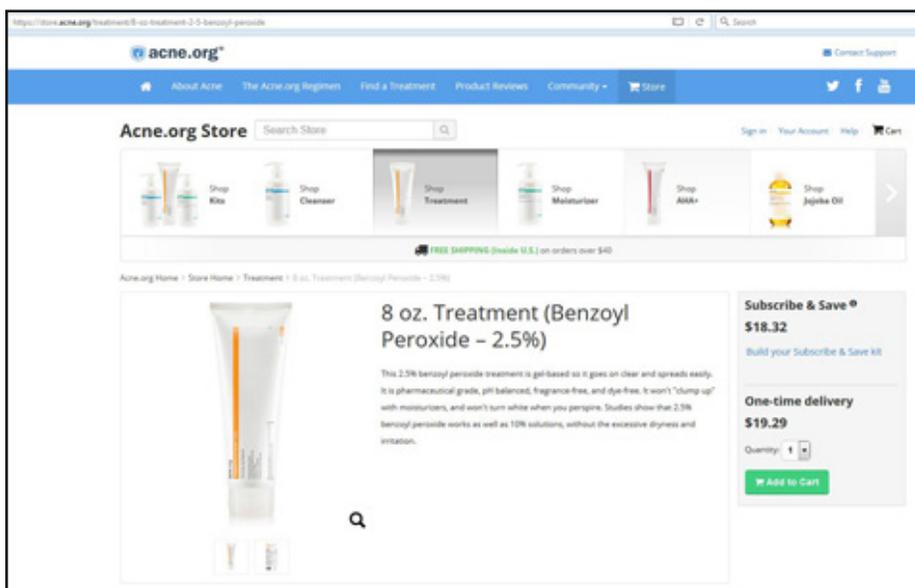
## **Attorneys:**

**Plaintiff:** Dominic V. Signorotti, Buchman Provine Brothers Smith LLP, Walnut Creek, CA

**Defendant:** Bonnie J. Wolf and Otto O. Lee, Intellectual Property Law Group LLP, San Jose, CA

## **Related Filing:**

Order: 2016 WL 6962954



**The defendant allegedly infringes the packaging of Mysfyt's 2.5 percent benzoyl peroxide treatment, which the company sells on Amazon.com and its website, Acne.org, shown here. The defendant sells his product mainly on Amazon.com, the suit says.**

## Hacker stole CostaRica.com, suit says

By Melissa J. Sachs

CostaRica.com Inc. has filed a Virginia federal lawsuit seeking to recover a domain the Central American travel company owned for more than 20 years until a hacker accessed the administrative settings and unlawfully transferred it.

**CostaRica.com Inc. et al. v. <costarica.com>, No. 16-cv-1465, complaint filed (E.D. Va. Nov. 25, 2016).**

The Costa Rica-based company initiated the cybersquatting action against its former domain, costarica.com, in the U.S. District Court for the Eastern District of Virginia, home of VeriSign Inc., the authoritative registry for .com generic top-level domains.

The Anticybersquatting Consumer Protection Act, 15 U.S.C.A. § 1125(d), allows parties to file a lawsuit against the domain name — so-called in rem actions — in the jurisdiction where the disputed domain name's registrar or registry sits if certain conditions are met.

In its complaint, CostaRica.com says its suit meets the conditions for an in rem action because the foreign travel company has U.S. common law rights to the domain name, which incorporates a "Costa Rica" trademark it has used for travel services since 1995.

The company also says recent records show the domain is currently registered to Amal Zakero, an individual in Egypt.

Because Zakero lacks the requisite contacts to face a lawsuit in the U.S., CostaRica.com says it must bring a U.S. suit in the registry's jurisdiction.

### 'POPULAR WEB DESTINATION'

CostaRica.com offers travel and tourism information about the Central American country.

The suit says the website has become popular among tourists because it has offered destination guides, weather updates and information on relocation and real estate in Costa Rica for more than 20 years.

Alejandro Solorzano-Picado, a Costa Rican resident, is an officer of the company and named as a co-plaintiff in the lawsuit.

According to the complaint, the plaintiffs have invested "tens of thousands of dollars" in the website's graphic design, development, search engine optimization and performance.

"Internet users and tourists have come to distinguish and recognize the legitimacy of plaintiffs' services as a result of this use and promotion," the suit says.

Although the complaint makes no reference to a U.S. federal trademark registration, it says the plaintiffs' activities show they own common law rights to "CostaRica.com" and "Costa Rica" marks.

### 'HACKED AND STOLEN'

In 2015 or 2016 a hacker unlawfully accessed CostaRica.com's administrative account with Melbourne IT, the previous registrar for the domain name, the suit says.

The hacker changed the administrative settings to forward all email and mail to addresses the plaintiffs did not own, the suit says.

After changing the contact details associated with the account, the hacker transferred the domain to its current registrar, Name.com Inc., which is located in Denver, the suit says.

The hacker also put a privacy service on the registration to hide details about who owned the domain, according to the complaint.

The plaintiffs did not learn of the theft until mid-2016 because the hacker never changed the website's nameserver, the technology that connects a domain to a website and determines what internet users see when they visit the URL, the suit says.

Because the nameserver stayed the same, the travel company's website content has remained active on the domain, according to the complaint.

Although the plaintiffs contacted the current registrar, they have been unable to reverse the fraudulent transfer, the suit says.

It seeks a court order to do that. **WJ**

#### Attorney:

Plaintiff: Steven Rinehart, Western IP Law, Salt Lake City, UT

#### Related Filing:

Complaint: 2016 WL 6993497

## Facebook's advertising metrics draw shareholder suit

By Eileen M. Potash

Facebook Inc. defrauded investors by failing to disclose that its advertising metrics contained errors that caused the social media company to overstate the success of its customers' paid advertising campaigns, according to a shareholder lawsuit filed in Nevada federal court.

***Nagy v. Facebook Inc. et al., No. 16-cv-2683, complaint filed (D. Nev. Nov. 22, 2016).***

The proposed class-action complaint says Menlo Park, California-based Facebook and its senior executives deceived investors by selling off millions of company shares when they discovered the faulty metrics. The executives also failed to disclose the errors for more than a year, until an analytics firm discovered miscalculations in Facebook's ad metrics in August.

Subsequently, Facebook announced Nov. 3 that it expected a "significant decrease" in its ad revenue, and the news sent the company's stock tumbling \$4 billion, according to the plaintiffs.

The lawsuit, filed Nov. 22 in the U.S. District Court for the District of Nevada, names as defendants Facebook, founder and CEO Mark Zuckerberg, Chief Financial Officer David Wehner, Chief Operating Officer Sheryl Sandberg, five other executives and one director.

Shareholder Aurangzeb Nagy and four other Facebook investors seek damages for shareholders who purchased and/or held Facebook stock during a 20-month class period ending Nov. 16.

### ADVERTISING METRICS

Facebook has made paid advertising a central component of its growth strategy, the plaintiffs allege.

In May 2014 the company introduced new advertising and content metrics designed to help advertisers measure how their online ads and campaigns perform on the social media website, the suit says.

However, Facebook failed to have a third party independently monitor or evaluate data compiled from the metrics or verify the accuracy of the results, the complaint claims.

Facebook allegedly discovered calculation errors in the metrics in April 2015 but failed to publicly disclose the information or mention it in Securities and Exchange Commission filings, according to the complaint.

### ALLEGED SELL OFF

After the discovery, Zuckerberg and the named Facebook executives started to sell a "substantial" number of their shares, the complaint says.

In September 2015 Facebook said it would let advertising companies use third-party software from analytics firm Moat Inc. to analyze their ad metrics on the website, the suit says.

Moat discovered a miscalculation in Facebook's metrics in August, and Facebook privately let its advertising customers know about the possible miscalculation, according to the complaint.

The following month, the social media company publically admitted it found an error in its video advertising metric but downplayed its significance, according to the plaintiffs.

When Facebook issued its quarterly statement Sept. 30, it made no mention of the faulty advertising metrics, the suit says.

### TRUTH REVEALED

On Nov. 3 Facebook announced it expects a significant decrease in ad revenue and growth in the upcoming year, according to the complaint.

Thereafter, Facebook's stock fell \$4 billion between Nov. 3 and Nov. 4, the complaint says.

The defendants allegedly violated the anti-fraud provisions of Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C.A. § 78j(b), and SEC Rule 10b-5, 17 C.F.R. § 240.10b-5.

Additionally, Zuckerberg and the other defendants are liable as control persons under Section 20(a) of the Exchange Act, 15 U.S.C.A. § 78t(a), the suit alleges. **WJ**

#### Attorneys:

*Plaintiffs:* Robert T. Eglet, Robert M. Adams and Erica D. Entsminger, Eglet Prince, Las Vegas, NV

#### Related Filing:

Complaint: 2016 WL 6943309



The lawsuit names Facebook CEO Mark Zuckerberg, shown here, as one of the defendants.

REUTERS/Stephen Lam

## DESIGN PATENT DEFEAT?



Richard M. LaBarge, a partner at Marshall, Gerstein & Borun based in Chicago, described the opinion as blunting the sword-edge that design patents afford to manufacturers.

The Federal Circuit's previous interpretation of Section 289 precluded considering other design or mechanical features when assessing damages, he noted.

"There was no dispute that other design features of the products, as well as mechanical features of those products, contributed to consumers' purchasing decisions, but U.S. design patent law does not require the same apportionment of damages that is used when assessing damages in a utility patent case," LaBarge said.



Christopher E. Loh, a partner in the New York office of Fitzpatrick, Cella, Harper & Scinto, said the decision could significantly reduce Apple's damages award.

"At the same time, however, the Supreme Court's decision leaves unresolved the practical question of how litigants and courts are to determine what components of a finished product should factor into a damages calculation under [Section 289]," he said.

"And the decision leaves open the possibility that, depending on the circumstances, the profits from a finished product in its entirety may still be an appropriate basis for calculating damages in design patent suits," he added.

## WHAT HAPPENS NEXT?



Beth Ferrill, a partner at the Washington office of Finnegan, Henderson, Farabow, Garrett & Dunner, said the Federal Circuit will likely develop a test that lower courts

may apply to determine the article of manufacture.

After the Federal Circuit decides what factors to consider with its test, it will likely pass the case back to the district court for another damages trial, she added.

"Today's decision only scratches the surface of resolving this case," she said. "The key sticking point at the district court will likely be how much of the profits from the smartphone should be attributed to the identified article of manufacture."



Mark S. Raskin, a partner at Mishcon de Reya New York LLP, expressed similar thoughts about the ongoing dispute.

"This decision will ultimately necessitate a new trial on damages," he said.

On a practical level, he added, a decision like this merely increases litigation costs.

"Litigants (and courts) are forced to stab blindly hoping to hit on an approach that might be approved by the Supreme Court some years and millions of dollars down the road," Raskin said.

## WHAT IS THE 'ARTICLE OF MANUFACTURE'?

This design patent dispute between the two smartphone manufacturers stems from a lawsuit Apple filed in 2011.

The complaint accused Samsung of multiple intellectual property violations, including infringement of U.S. Patent Nos. D618,677; D593,087; and D604,305, design patents covering elements on the face of Apple's iPhone.

After years of litigation and a jury trial, the case came before the Federal Circuit, which affirmed a \$399 million award that Apple won for Samsung's design patent infringement. *Apple Inc. v. Samsung Elecs. Co.*, 786 F.3d 983 (Fed. Cir. 2015).

Samsung filed a certiorari petition in December 2015, saying the Federal Circuit affirmed a miscalculated award.

Apple collected all profits from sales of the allegedly infringing product, smartphones sold to consumers, rather than a "portion of

the product to which the patented design is applied," Samsung said.

By interpreting "article of manufacture" to mean an entire product, the Federal Circuit incorrectly affirmed Apple's windfall, despite all the other patented components in a smartphone, Samsung said.

The high court agreed in March to resolve the dispute.

## ENTIRE PRODUCT OR COMPONENT?

During October's oral argument, Samsung argued that infringing design patents covering a smartphone's rounded edges, bezel and graphical user interface should not result in an award of total profits from the phones' sales.

Apple argued the nearly \$400 million award was proper for Samsung's infringement of the three relevant design patents, which previously gave iPhones a distinctive and pleasing appearance.

At the argument, Apple also conceded the relevant article of manufacture does not always have to be the final product.

However, Samsung had the opportunity to put forth evidence that showed the article of manufacture was something less than the entire product, and the company's expert chose to use the end product sold to consumers to calculate damages, Apple said.

The U.S. government stepped in as a friend of the court and offered a test to help determine the relevant article of manufacture.

## MAY BE BOTH, BUT NO OTHER GUIDANCE

In its nine-page decision, the high court refrained from articulating any sort of test to help determine the relevant article of manufacture in future cases.

The justices said the parties had not adequately briefed the issue and that devising a test was unnecessary to resolve the question presented in the case.

Instead, the high court offered examples of the way the term "article of manufacture" has been interpreted in other parts of the Patent Act.

For instance, the Patent Office and courts have understood the term to cover "a component of a multicomponent product"

when applying Section 171(a) of the Act, 35 U.S.C.A. § 171(a), which explains what is eligible for design patent protection, the court said.

"Thus, reading 'article of manufacture' in Section 289 to cover only an end product sold to a consumer gives too narrow a meaning to the phrase," the court concluded.

It deferred to the Federal Circuit to resolve this issue on remand. [WJ](#)

(Additional reporting by Patrick H.J. Hughes)

**Attorneys:**

*Petitioners:* Kathleen M. Sullivan, Quinn Emanuel Urquhart & Sullivan, New York, NY

*Respondent:* Seth P. Waxman, Wilmer Cutler Pickering Hale & Dorr, Washington, DC

**Related Filing:**

Opinion: 2016 WL 7078449

**See Document Section A (P. 21) for the opinion.**



WESTLAW JOURNAL  
**CLASS ACTION**

This newsletter gives you information on recent developments in class action litigation.

Call your West representative for more information about our print and online subscription packages, or call 800.328.9352 to subscribe.

## NEWS IN BRIEF

### POLISH TV CREATOR CANNOT STREAM LICENSED SHOWS TO US, COURT SAYS

Poland's national public television broadcasting company infringed the U.S. copyrights of 51 Polish shows it created by streaming them online after giving a Canadian company exclusive distribution rights in North and South America, a federal court has ruled. Ontario-based Spanski Enterprises Inc. presented evidence that Telewizja Polska SA intentionally turned off geoblocking, a feature that should have prevented U.S.-based IP addresses from accessing the 51 shows, U.S. District Judge Tanya S. Chutkan of the District of Columbia said. Spanski witnesses testified they could access the licensed copyrighted content from TVP Polonia, Telewizja Polska's international channel, in the U.S. without using a proxy server or virtual private network that could trick geoblocking technology, the judge said. There was also evidence that for a U.S.-based IP address to gain access to the copyrighted shows, the geoblocking system would have to fail or a TVP employee would have to commit an intentional act, she said. Based on this evidence, the judge granted Spanski's summary judgment motion on the infringement claims.

***Spanski Enterprises Inc. v. Telewizja Polska SA, No. 12-cv-957, 2016 WL 7030970 (D.D.C. Dec. 2, 2016).***

**Related Filing:**

Opinion: 2016 WL 7030970

### REINSURER SCORES SCOREINSURANCE.COM DOMAIN

The World Intellectual Property Organization has taken the domain scoreinsurance.com from a South Carolina registrant and awarded it to French reinsurer Scor SE. The addition of the letter "e" and the generic term "insurance" did not prevent the domain from being confusingly similar to the insurer's "Scor" trademark, the WIPO panel said. Julius Thomas Jr. of Columbia, South Carolina, who registered scoreinsurance.com in April, failed to explain why he chose to register that domain or say what rights he might have to it, the panel said. According to the decision, Thomas worked in the fitness industry, not insurance, and the domain contained sponsored links and pay-per-click advertisements for Scor's competitors. Paris-based Scor is the world's fifth-largest reinsurance company, according to the decision. It holds Scor trademark registrations for reinsurance in several countries, including the U.S., the panel added. Given Scor's fame in the insurance industry, it is "inconceivable" Thomas registered the domain without knowledge of the company or its mark, the panel concluded.

***Scor SE v. Thomas et al., No. D2016-1977, 2016 WL 6947276 (WIPO Arb. Nov. 24, 2016).***

**Related Filing:**

Decision: 2016 WL 6947276

### CERTIFICATION MARK HOLDER OPPOSES SCHOOL'S HIGH COURT PETITION

A data security certification group says in a Supreme Court brief that its dispute with a for-profit cybersecurity school would make a poor vehicle for setting a standard to determine when using another party's trademark qualifies as a nominative fair use. The 2nd U.S. Circuit Court of Appeals decision that Security University LLC asked the high court to review concerns a certification mark, which is different than a traditional trademark, nonprofit International Information Systems Security Certification Consortium says in its opposition brief. The distinction between these two marks was foundational to the 2nd Circuit's nominative fair use analysis and its ruling that Security University failed to show the school's use of the nonprofit's certification marks was permitted, the opposition brief says. Security University contests the 2nd Circuit's 11-part nominative fair use test, which combines elements from other circuits, necessarily creating a circuit split, according to the school. However, no other circuit has considered the issue for a certification mark, so there can be no split among the federal appeals courts, the nonprofit says.

***Security University LLC et al. v. International Information Systems Security Certification Consortium Inc., No. 16-352, opposition brief filed (U.S. Nov. 18, 2016).***

**Related Filings:**

Opposition brief: 2016 WL 6493173

Certiorari petition: 2016 WL 5048645

## CASE AND DOCUMENT INDEX

---

<i>BMG Rights Management (US) LLC v. Cox Communications Inc. et al.</i> , No. 16-1972, <i>brief filed</i> (4th Cir. Nov. 14, 2016).....	7
<i>CostaRica.com Inc. et al. v. &lt;costarica.com&gt;</i> , No. 16-cv-1465, <i>complaint filed</i> (E.D. Va. Nov. 25, 2016) .....	14
<i>Edmondson et al. v. Velvet Lifestyles LLC et al.</i> , No. 15-cv-24442, 2016 WL 7048363 (S.D. Fla. Dec. 5, 2016) .....	10
<b>Document Section C</b> .....	38
<i>Impression Products Inc. v. Lexmark International Inc.</i> , No. 15-1189, 2016 WL 1117396, <i>cert. granted</i> (U.S. Dec. 2, 2016) .....	6
<i>Medical Marijuana Inc. et al. v. ProjectCBD.com et al.</i> , No. D068523, 2016 WL 6835522 (Cal. Ct. App., 4th Dist., Div. 1 Nov. 21, 2016) .....	8
<b>Document Section B</b> .....	28
<i>Mysfyt Inc. v. Lum</i> , No. 16-cv-3813, 2016 WL 6962954 (N.D. Cal., Oakland, Nov. 29, 2016).....	13
<i>Nagy v. Facebook Inc. et al.</i> , No. 16-cv-2683, <i>complaint filed</i> (D. Nev. Nov. 22, 2016).....	15
<i>Nix et al. v. Major League Baseball et al.</i> , No. 159953/2016, <i>complaint filed</i> (N.Y. Sup. Ct., N.Y. Cty. Nov. 28, 2016) .....	11
<i>Reynolds v. State</i> , No. 06-15-194, 2016 WL 6995033 (Tex. App., Texarkana Nov. 30, 2016).....	12
<i>Samsung Electronics Co. et al. v. Apple Inc.</i> , No. 15-777, 2016 WL 7078449 (U.S. Dec. 6, 2016) .....	1
<b>Document Section A</b> .....	21
<i>Scor SE v. Thomas et al.</i> , No. D2016-1977, 2016 WL 6947276 (WIPO Arb. Nov. 24, 2016).....	17
<i>Security University LLC et al. v. International Information Systems Security Certification Consortium Inc.</i> , No. 16-352, <i>opposition brief filed</i> , (U.S. Nov. 18, 2016) .....	17
<i>Spanski Enterprises Inc. v. Telewizja Polska SA</i> , No. 12-cv-957, 2016 WL 7030970 (D.D.C. Dec. 2, 2016) .....	17