ITC Section 337 Update

Jeffrey M. Telep

King & Spalding LLP

Fifth Annual "Live at the ITC"

On July 30, 2014, the Fifth Annual Forum on Section 337 and Other Developments at the U.S. International Trade Commission, entitled "Live at the ITC," was co-sponsored by the ABA-IPL Section ITC Committee, the ITCTLA and the D.C. Bar International Law Section and hosted in King and Spalding's Washington, DC offices. Highlights of the forum included an intimate Q and A session with ITC Chairman Meredith Broadbent, Vice Chairman Dean Pinkert, Former Chairman and current Commissioner Irving Williamson and more recently appointed Commissioners David Johansson and Scott Kiefe, who discussed their new experience as commissioners. Other topics and questions covered by the commissioners included the issue of public interest, with Chairman Broadbent noting that since 2010, the issue of public interest has been delegated to the ALJ for fact finding in 38 investigations, 5 of which have reached a final determination, and 12 are still pending. Although the 100-Day ID Procedure has only been used in one investigation to date, Commissioner Williamson stated that the Commission is not hesitant to use it in the right case. Margaret Macdonald, Director of OUII, reviewed the criteria for staff to have full, partial or no participation in an investigation and encouraged complainants to respond to public interest statements filed by respondents and the public. Finally, a panel of practitioners addressed non-traditional uses of Section 337, emphasizing that injury must be shown in investigations not involving traditional patent, registered trademark and/or copyright infringement issues.

Domestic Industry Is Not Satisfied Based Solely On Licensees' Expenditures When License Is Purely Revenue Driven

ALJ Lord issued an "Initial Determination" ("ID") in *Certain Optical Disc Drives, Components Thereof, And Products Containing The Same*, Inv. No. 337-TA-897, granting motions for summary determination on lack of domestic industry and terminating the investigation in its entirety. The ID held that a licensing entity whose patent-related activities are purely revenue driven cannot choose to prove the existence of the economic prong of a domestic industry entirely through its licensees' activities under subsections (A) and (B) of section 337(a)(3), essentially avoiding the requirements of subsection (C), which requires evidence of a revenue-driven licensing entity's own patent-related activities and expenditures. *See, e.g., Certain Multimedia Display and Navigation Devices and Systems, Components Thereof, and Products Containing the Same*, Inv. No. 337-TA-694, Corrected Comm'n Op. (Aug. 8, 2011). The complainant, Optical Devices, made no attempt to prove any domestic expenditures of its own, arguing that it had no obligation to show such expenditures when relying exclusively on the activities of its licensees to argue that a domestic industry relating to the asserted patents exists. ALJ Lord determined that complainant's reliance on its licensees activities to prove the economic prong of domestic industry through purely revenue-driven licenses failed to comport with case law construing section 337(a)(3), including *Schaper Manufacturing Co. v. Int'l Trade Comm'n*, 717 F.2d 1368 (Fed. Cir. 1983), which found a domestic industry where licensees engage in domestic activities under licenses that relate to development or production of patented articles.

Jeffrey M. Telep

Commission Upholds Its Prior Precedent That APO Petitioner Carries The Burden Of Proving Non-infringement

In an Advisory Opinion issued on August 11, 2014 in *Certain Sleep-Disordered Breathing Treatment Systems*, Inv. No. 337-TA-879, the Commission found the Supreme Court's holding in *Medtronic v. Mirowski,* 134 S. Ct. 843 (2014), that the burden of proving infringement in a declaratory judgment action remains with the patent owner, does not apply to an Advisory Opinion Proceeding ("APO") under Commission Rule 210.79. The Commission reversed the ALJ's decision to place the burden of proving infringement on the patentee, ResMed, in view of the Supreme Court's decision in *Medtronic,* in the APO requested by Apex. The Commission adopted, with modified reasoning, the ALJ's findings that Apex's redesigned iCH humidifier is covered and Apex's redesigned WIZARD 220 is not covered by the Consent Order and reversed the ALJ's finding that Apex's redesigned XT humidifier is covered by the Consent Order issued by the Commission in the underlying investigation. The Commission distinguished the Supreme Court's legal and practical considerations on the burden of proof issue, finding, *inter alia*, that "in APOs, the patent owner is not necessarily in a better position to bear the burden of proof because the issues of patent scope and infringement of the original, accused products usually have already been determined in the underlying investigation. In such cases, the respondents are able to point out, how and why their redesign is different from the litigated products and does not infringe."

Federal Circuit Decides Not To Address *En Banc* Joint Infringement Issue

On July 24, 2014, the Federal Circuit s*ua sponte* rejected Akamai's request and the Supreme Court's suggestion that the Federal Circuit can decide the issue of joint infringement *en banc* if it chooses to do so in *Akamai v. Limelight*, Appeal No. 2009-1372. Instead, the Federal Circuit decided to refer the case on remand to its "two remaining panel members and a newly selected judge." The Federal Circuit had granted Akamai's request to review the issue of joint infringement in 2011, but never reached this issue. Rather, the *en banc* Federal Circuit found that Limelight, who does not perform the claim step of tagging components to be stored on its servers, which Limelight requires its customers to do, was liable for induced infringement because inducement can be found even when there is no single entity that directly infringes by performing all steps of a method claim. As reported in ITC Section 337 Update dated July 18, 2014, the Supreme Court reversed this decision, finding that induced infringement cannot be found when no single entity performs all steps of the method claim. Akamai subsequently requested the Federal Circuit to revisit *en banc* the issue of whether joint performance of a patented method can create liability for direct infringement. Limelight argued that Akamai failed to preserve the issue of whether the Federal Circuit's standard for joint infringement set forth in *Muniauction v. Thomson*, 532 F.3d 1318 (Fed. Cir. 2008) was wrong.

Jeffrey M. Telep, *resident in the firm's Washington, D.C. office****,*** *is a Partner in King & Spalding's International Trade Group. He has over 20 years of experience litigating high-profile international trade remedy disputes, specifically unfair trade practice investigations under Section 337 of the Tariff Act of 1930, antidumping and countervailing duty investigations under the Tariff Act, Customs fraud investigations, seizures and forfeitures, and other commercial disputes.*

Please email the author at jtelep@kslaw.com with questions about this article.

Russian Hackers Stockpile Over One Billion Internet Credentials

Phyllis B. Sumner
Sarah E. Statz
Elizabeth K. Hinson

King & Spalding LLP

A Russian hacking group reportedly engaged in the largest-known cyber attack by amassing over 1.2 billion unique sets of usernames and passwords and 500 million e-mail addresses from more than 420,000 web and FTP sites. The attack was uncovered by Hold Security, an information security company based in Milwaukee, which has been investigating the attack for several months. Various news reports have confirmed the company's findings.[1] Among the victims are "leaders in virtually all industries across the world,"[2] including "the auto industry, real estate, oil companies, consulting firms, car rental businesses, hotels, computer hardware and software firms and the food industry," but Hold Security is not naming specific victims.[3] The security firm intends to reach out to individual victims confidentially.[4] The Russian hackers reportedly utilized a hacking technique known as a SQL injection, which exploits a security vulnerability in an application's software to inject malicious code.[5]

Phyllis B. Sumner

Sarah E. Statz

Elizabeth K. Hinson

Companies that are victims of the cyber attack that collect information from California and Florida residents may have an obligation under those state data breach notification laws to notify affected individuals and government agencies. In California and Florida, personally identifiable information includes an email address or username in combination with a password, among other data elements. If consumer usernames or email addresses and passwords were stolen by the Russian hackers, companies that collect that information from California or Florida residents may have a duty to notify the consumers and report the breach to government authorities.

In addition, even the state data breach notification laws that do not define personal information to include usernames and passwords may be implicated if there is evidence that the hackers use the stolen usernames and passwords to gain access to a consumer's account and are able to obtain additional personal identifying information about the consumer from the website. For example, the hackers could use the login information to gain access to the user's account information, including potentially the consumer's name, date of birth, address or account numbers. Although there are no reports that the hackers have used the username and password information to gain access to additional personal identifying information available on the websites, if that activity is suspected, entities may have an obligation under state data breach laws to notify consumers.

This massive attack highlights the need for increased website security across all industries. Companies should no longer rely on "trusted" web applications to adequately protect their information. Instead, companies should focus on implementing their own network defenses. Website managers should immediately start testing their sites for intrusions and update any patches available for their web servers, database servers and applications. Clients should also contact third-party service providers to ensure that those vendors are monitoring for fraud and updating any security patches. Clients should take proactive measures immediately, such as performing a risk analysis to assess potential risks to the personally identifiable information they collect and maintain. Clients should ensure that they collect only data that is necessary and adopt technical measures to protect data, including encryption or suitable hashing mechanism. Clients should also update privacy policies and procedures, and implement procedures to identify and respond to breach events.

Phyllis B. Sumner *is a Partner in King & Spalding's Business Litigation Practice Group in Atlanta. She represents clients in a variety of complex litigation matters involving, among other subjects, commercial disputes, False Claims Act, information ptivacy and security, Fair Credit Reporting Act, RICO, securities and fraud, and provides counsel on a variety of corporate matters.* ***Sarah E. Statz*** *and* ***Elizabeth K. Hinson(Bess)*** *are Associates in King & Spalding's Atlanta office, and Sarah is and a member of the firm's Business Litigation Practice Group. For the footnotes to this article, go to http://www.metrocorpcounsel.com/articles/29845/russian-hackers-stockpile-over-one-billion-internet-credentials.*

Please email the authors at psumner@kslaw.com, sstatz@kslaw.com or bhinson@kslaw.com with questions about this article.