King & Spalding

Intellectual Property Newsletter

July/August 2015

In This Issue

King & Spalding News

Protecting Trade Secrets in the Era of the Data Breach

Steven Snyder

The prevalence of data breaches cannot be ignored. New data breaches continue to occur one after another. In the first half of 2015 alone there were reports of large scale data breaches involving multiple companies in the healthcare industry, the United States Office of Personnel Management (OPM), the IRS, a telecommunications provider, an online console gaming provider, and a transportation company.[i] Organizations face a monumental task of safeguarding confidential data, as the concept of a safe perimeter around private networks continues to erode and adversaries become ever more sophisticated.[ii] While efforts and failures to secure data have received a large amount of press, most of it has been focused on breaches relating to information about people—whether financial or medical.[iii] This is primarily because most of the laws that relate to liability for data breaches in the U.S. deal with identifiable information relating to individuals.[iv] In addition, the thought of peoples' private information being stolen or disclosed invokes a strong emotional reaction from the public that a breach of other business data does not.

Nevertheless, companies should be equally concerned about the breach of non-personal business data, such as their trade secrets, and establish proper safeguards to mitigate the attendant risks. The Uniform Trade Secret Act identifies a trade secret as follows:[v]

(4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

As this definition shows, to qualify as trade secrets, two primary requirements must be met; 1) the information derives value by being kept confidential, and 2) the company must take reasonable steps to maintain the secrecy of the information. Unlike other types of IP protection such as patents and copyrights, which protect information after it is made public, trade secret law protects valuable information that the company endeavors to keep secret. The remedies available to organizations that comply with these trade secret requirements include criminal punishments in the event of theft,[vi] as well as injunctions to prevent the information from being used improperly-such as in the importation of a competing product.[vii]

Securing Trade Secrets

The trade secret definition counsels that even if business data is valuable if kept secret, it does not qualify as a trade secret unless the organization takes efforts that are *reasonable under the circumstances* to maintain the secrecy of the data.[viii] Companies should therefore consider trade secrets law requirements at the outset of the process of designing or updating their information security programs.

The following suggestions, which are consistent with implementing a cybersecurity framework such as the NIST Cybersecurity Framework,[ix] can help insure that trade secrets are identified and appropriately protected:

- **Prioritize Objectives and Define Scope of Assets:** In this step, the organization should consider the role of trade secrets in the organization or business line. Here, business objectives and how those objectives are supported by trade secrets should be specifically considered along with all other data assets.

- **Orient:** This step involves establishing an overall organizational risk approach including identifying threats and vulnerabilities to the systems related to the trade secrets and other data. The risks of loss of business value of trade secrets should be considered in conjunction with risks associated with loss of other types of data such as personal financial information.

- **Risk Assessment:** The unique aspects of trade secrets should be considered in conducting the risk assessment. The analysis should consider the possible post-breach protections, discussed below, which may mitigate the harm caused by the disclosure as long as reasonable steps were taken to avoid the breach.

- **Implementation:** An organization must prioritize the action plan that is intended to address gaps between the current cybersecurity profile of the organization and the target profile. The preceding suggestions will help to prioritize the action plan to insure the actions taken to secure the trade secrets are deemed reasonable as required to preserve the trade secret status.

Preparing for a Breach

Ideally, of course, a company that takes reasonable steps to secure its trade secrets would not have to worry about a data breach and be confident that its information is 100% secure. Sadly, this is not the world we live in. Organizations are being assailed by all levels of attacks including advanced persistent threats sponsored by nation states.[x] In view of the fact that those securing a network have to be successful 100% of the time, while those trying to breach it only have to be successful once, the deck is stacked against perfect security. Therefore, an organization must consider not just how to take reasonable measure to secure trade secrets, but it must tailor its incident response plan in the event that trade secrets are misappropriated despite its reasonable efforts to secure them.

Incident response plans should include measures to preserve information to identify the source of breaches.[xi] This information can assist in both criminal and civil proceedings against those responsible. As previously mentioned, there are criminal penalties for theft of trade secrets in the U.S.[xii] Criminal prosecutions may help provide a deterrent and could potentially stop a trade secret from being disseminated if the perpetrator was caught prior to disclosing the trade secret. Unfortunately, recent statistics suggest only 18% of breaches originate in the U.S. where the perpetrators would be subject to prosecution domestically.[xiii] International prosecution is possible but much more complex for obvious reasons.[xiv] In most cases, therefore, the entity responsible for the breach will not be subject to prosecution and, if the trade secrets are disseminated, prosecution of an individual may not provide the organization much recompense.[xv] Civil actions are similarly limited due to inability to reach many foreign adversaries and individuals not being able to make a company whole for the loss suffered even if the individual is subject to jurisdiction for civil suit.

If a company suffers a breach including loss of trade secrets and identifies the perpetrators as outside of the U.S., the company should consider setting up a monitoring program for imported goods that encompass its trade secrets. Assuming the company took reasonable steps to protect the trade secrets prior to the breach, it may be able to get an injunction to prevent the importation of goods utilizing its proprietary information.[xvi] This will be a difficult endeavor, but for a company with highly valuable trade secrets, such vigilance may be the only meaningful choice in many situations.

---

[i] *See* Insurance Giant Anthem Hit by Massive Data Breach (Feb. 4, 2015), *available at* http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/, Premera Blue Cross Breach Exposes Financial, Medical Records (Mar. 17, 2015) *available at* http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/, U.S. Intelligence Chief James Clapper Suggests China Behind OPM Breach (June 25, 2015) *available at* http://www.wsj.com/articles/SB1000711158351184369540458106986317089950 4, IRS Believes Massive Data Theft Originated in Russia (June 4, 2015) *available at* http://www.cnn.com/2015/05/27/politics/irs-cyber-breach-russia/index.html, Third Xbox Hacker Pleads Guilty (Jan. 21, 2015) *available at* http://www.consumeraffairs.com/news/third-xbox-hacker-pleads-guilty-012115.html, Uber Suffers Data Breach Affecting 50,000 *available at* http://www.forbes.com/sites/davelewis/2015/02/28/uber-suffers-data-breach-affecting-50000/, Order, *In the Matter of AT&T Services, Inc.*, FCC DA 15-399 (Apr. 8, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf.

[ii] *See generally* Verizon 2015 Data Breach Investigations Report ("2015 VBIR"), available at http://www.verizonenterprise.com/DBIR/2015/.

[iii] *See e.g.*, n. i, *supra*.

[iv] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 Pub. L. No. 104-191, 100 Stat. 2548 (medical records), The Children's Online Privacy Protection Act (15 U.S.C. §§ 6501-6506) (children under 13), Gramm-Leach-Bliley Act 12 CFR §1016 (consumer financial information), Fair Credit Reporting Act (consumer credit information); Section 5 of the Federal Trade Commission Act. (FTC Act) (15 U.S.C. §45) (protecting consumers).

[v] *See* Uniform Trade Secrets Act at 5 (http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf).

[vi] *See, e.g.*, Theft of Trade Secrets, 18 U.S.C. § 1832.

[vii] *See, e.g.*, Unfair Practices in Import Trade, 19 U.SC. § 1337; *see also TianRui v. U.S. International Trade Commission*, 661 F.3d. 1322, 1324 (Fed. Cir. 2011).

[viii] See trade secret definition, p.1 *supra*.

[ix] *See* Implementing the NIST Cybersecurity Framework, 2014 (available from ISACA); see also generally NIST Cybersecurity Framework).

[x] *See generally* 2015 VBIR.

[xi] *See* Incident Response Plan Example, State of California *available at* http://www.cio.ca.gov/ois/government/library/documents/incident_response_plan_example.doc

[xii] See Theft of Trade Secrets, 18 U.S.C. § 1832.

[xiii] 2013 Verizon Data Breach Report, *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[xiv] *See* Third Xbox Hacker Pleads Guilty (Jan. 21, 2015) available at http://www.consumeraffairs.com/news/third-xbox-hacker-pleads-guilty-012115.html.

[xv] *See e.g.*, *id.* (costs estimated at between $100 million and $200 million while only $650,000 in cash and proceeds was seized).

[xvi] *See, e.g.*, Unfair Practices in Import Trade, 19 U.SC. § 1337; *see also TianRui v. U.S. International Trade Commission*, 661 F.3d. 1322, 1324 (Fed. Cir. 2011).

Commil v. Cisco – Supreme Court Weighs in on Inducement

Thomas J. Gray/Christopher C. Carnaval

After taking a significant interest in patent law last term, the U.S. Supreme Court has again waded into the patent waters, this time to decide, as a matter of first impression, whether a good faith belief that a patent is invalid is a defense to inducement liability under 35 U.S.C. § 271(b). On May 26, 2015, the Court, in a 6-2 decision, ruled that such a defense does not exist.

Section 271(b) states that "[w]hoever actively induces infringement of a patent shall be liable as an infringer." A finding of inducement requires an underlying act of direct infringement. It further requires that the accused inducer had knowledge of the existence of the infringed patent and, as recently held by the Supreme Court in Global-Tech Appliances Inc. v. SEB S.A., "knowledge that the induced acts constitute patent infringement." It is not enough that an inducer intentionally causes another to engage in conduct that happens to amount to infringement; it must know, either actually or through willful blindness, that the intended conduct constitutes patent infringement.

In Commil USA LLC v. Cisco Systems Inc., a divided U.S. Court of Appeals for the Federal Circuit panel held that "evidence of an accused inducer's good-faith belief of invalidity may negate the requisite intent for induced infringement." Commil had alleged that Cisco, through sales of Wi-Fi access points and controllers, induced its customers to infringe Commil's patent related to a method of providing handoffs of mobile devices from one base station to another. After a jury trial, Cisco was found liable for inducement. Cisco appealed to the Federal Circuit on multiple grounds, most notably, that the district court erroneously precluded Cisco from presenting evidence of its good faith belief of invalidity to show that it lacked the requisite intent to induce infringement.

In concluding that the district court erred in excluding Cisco's evidence of its good faith belief of invalidity, the Federal Circuit noted that, while not having previously addressed the question with respect to a good faith belief of invalidity, it was well-established that "a good-faith belief of non-infringement is relevant evidence that tends to show that an accused inducer lacked the intent required to be held liable for induced infringement." The court saw no principled distinction between a good faith belief of invalidity and a good faith belief of non-infringement. Accordingly, because "one cannot infringe an invalid patent," an alleged inducer could hardly be said to have intended to induce infringement of a patent that it in good faith believed was invalid. (Of course, because there can be no liability for infringement of an invalid patent, an alleged inducer's good faith belief of invalidity only matters when it is incorrect.)

Both parties petitioned the Supreme Court for review of various parts of the Federal Circuit opinion, and the Supreme Court granted certiorari on this issue alone. Essentially, the Court was tasked with clarifying the meaning of "infringement" as used in § 271(b) and the Global-Tech holding. Does "knowledge that the induced acts constitute patent infringement" mean "knowledge that the induced conduct would result in liability for infringement" or "knowledge that the induced conduct meets all the limitations of a patent claim regardless of ultimate liability?"

As an initial matter, the Court, in an opinion delivered by Justice Kennedy, reaffirmed its explicit holding in Global-Tech "that liability for induced infringement can only attach if the defendant knew of the patent and knew as well that 'the induced acts constitute patent infringement.'" In other words, mere knowledge of the patent alone is not enough. Interestingly, though it was not the question before the Court, Commil (supported by the Government) devoted more than half of its brief arguing that satisfaction of the intent requirement requires merely that an alleged inducer have knowledge of a patent and its potential relevance to the alleged inducer's activities (such as through a notice letter from the patentee alleging infringement). Under this view, a defendant's subjective beliefs about any potential defenses, including both invalidity and non-infringement, are irrelevant to the intent analysis. The Court, along with dissenting Justice Scalia and Chief Justice Roberts, squarely rejected this theory as contrary to the clear language and sound rationale of Global-Tech.

Moving to the question before it, the Court held that a defendant's belief regarding patent validity is not a defense to a claim of induced infringement. The Court reasoned that a belief of invalidity cannot negate the scienter required under § 271(b) – intent to "bring about the desired result," i.e., infringement – because infringement and validity are separate and distinct legal issues that are to be determined independently. In particular, the Court noted that infringement and validity appear in separate parts of the Patent Act and non-infringement and invalidity are listed as two separate defenses. Each bears its own burdens, presumptions and evidence. Interpreting § 271(b) as permitting a defense of belief in invalidity would, according to the Court, conflate the two legal issues. The Court further reasoned that such a defense would also drastically undermine the statutory presumption of patent validity, which requires invalidity to be proven by clear and convincing evidence and not by an accused infringer's own subjective belief. Judge Scalia disagreed. In his dissenting opinion, he wrote, "An alleged inducer who succeeds in this defense does not thereby call a patent's validity into question. He merely avoids liability for a third party's infringement of a valid patent, in no way undermining that patent's presumed validity."

Underlying the Court's ruling is the notion that a patent claim can be infringed regardless of its validity, the difference being that infringement of a valid claim results in liability while infringement of an invalid claim does not. The Court explained that questions of infringement and validity require "a determination of the procedures and sequences that the parties must follow to prove that act of wrongful inducement and any related issues of patent validity" and that "the allocation of the burden to persuade on these questions, and the timing for the presentations of the relevant arguments, are concerns of central relevance to the orderly administration of the patent system." As such, "invalidity is not a defense to infringement, it is a defense to liability." If a patent is indeed invalid, and is proven to be so under proper procedures, there is no liability even for an infringed patent.

Justice Scalia, in his dissent, responded to this reasoning by noting that "[i]nfringing a patent means invading a patentee's exclusive right to practice his claimed invention." Because only valid patents confer this right to exclusivity, only valid patents can be infringed. And because only valid patents can be infringed, "anyone with a good-faith belief in a patent's invalidity necessarily believes the patent cannot be infringed. And it is impossible for anyone who believes that a patent cannot be infringed to induce actions that he knows will infringe it."

Cisco had made a similar argument that Global-Tech and § 271(b) require specific, culpable intent, i.e., knowledge of wrongdoing or unlawful conduct in violation of a patentee's rights. There is nothing wrong or unlawful about practicing an invalid patent claim. It follows, then, that an alleged inducer with a reasonable, good faith belief that a patent claim is invalid cannot be found to have induced infringement because it would not have knowingly and intentionally encouraged wrongful conduct in violation of the patentee's rights. In this regard, distinctions between a good faith belief of invalidity and a good faith belief of non-infringement do not matter. The Court, however, drew from the laws of trespass and tortious interference with a contract, for the proposition that an act may be "intentional" for purposes of civil liability, even though that actor lacked actual knowledge that its conduct violated the law. Similarly, under the Court's ruling, an accused infringer may be found liable for induced infringement even if it has no knowledge that the acts it induced violate a patentee's rights.

Overall, the Supreme Court's Commil decision may be a mixed result for accused infringers. On the one hand, they may no longer rely on a good faith belief in invalidity as a defense to a claim of inducement. On the other hand, the Court reaffirmed its holding in Global-Tech that inducement requires knowledge of the patent and knowledge that the induced acts meet each and every limitation of the asserted patent claims.

King & Spalding News

King & Spalding Achieves Important Appellate Victory for Pandora Media

NEW YORK, May 8, 2015 — King & Spalding achieved an important appellate victory on May 6 on behalf of Pandora Media in the company's licensing dispute with the American Society of Composers, Authors and Publishers (ASCAP). The U.S. Court of Appeals for the Second Circuit in Manhattan rejected ASCAP's appeal of a lower court ruling that ensured Pandora's access to the catalogs of certain ASCAP publisher members under Pandora's blanket license agreement with ASCAP, notwithstanding those publishers' efforts to restrict such access. The lower court also had set a reasonable rate for Pandora's use of ASCAP music after a lengthy bench trial, and the Second Circuit affirmed that ruling as well, rejecting ASCAP's demand for a much higher rate.

The dispute arose after the world's two largest music publishers, Sony/ATV and Universal, attempted to selectively withdraw "new media" licensing rights from ASCAP in order to require Pandora to negotiate public performance licenses for those publishers' works directly with the publishers (as opposed to securing a blanket license through ASCAP). ASCAP nevertheless retained the right to license the "withdrawing" publishers' works to the vast majority of music users. By so "withdrawing," the publishers wished to circumvent the effective compulsory license and court rate oversight provisions of ASCAP's consent decree with respect to certain "new media services" (while retaining the benefits of collective licensing through ASCAP for the vast majority of licensees).

Citing Pandora's application for a license through 2015 under ASCAP's consent decree—which unambiguously requires ASCAP to grant any music user a license to perform all of the works in its repertory—Pandora sought a court ruling confirming that these publisher withdrawals could not impact the company's access to the entire ASCAP repertory, inclusive of the catalogs of the "withdrawing" publishers. In October 2013, Pandora, represented by King & Spalding, obtained a favorable summary judgment ruling on this issue in district court. The Second Circuit affirmed that decision on May 6.

"The licensing of works through ASCAP is offered to publishers on a take-it-or-leave-it basis," the Second Circuit wrote in its opinion. "As ASCAP is required to license its entire repertory to all eligible users, publishers may not license works to ASCAP for licensing to some eligible users but not others."

The publishers' attempt to leverage their size to extract higher rates from Pandora in direct licenses by selectively withdrawing their works from ASCAP thus was legally invalid. The decision has industry-wide implications, as it applies to all ASCAP licensees. The Second Circuit's affirmance of the rate set by the district court also is of significant economic benefit to Pandora (and likely other similar digital music services).

Pandora was represented in this matter by King & Spalding intellectual property partners Kenneth Steinthal and Joe Wetzel, who both are based in the firm's San Francisco office and who led the victorious trial team, as well as appellate litigation partner Jeffrey Bucholtz (Washington, D.C.), who argued the case in the Second Circuit. Other members of the cross-office Pandora team include associates Blake Cunningham (Austin), Katy Merk and Ethan Davis (San Francisco) and David Mattern (Washington, D.C.).

King & Spalding's full-service intellectual property practice combines proven first-chair trial and business lawyers with true industry specialists. It consists of more than 90 IP professionals, including more than 80 lawyers, agents and technical advisors with technical degrees, located in the firm's offices in Atlanta, Austin, Charlotte, Houston, Moscow, New York, San Francisco, Silicon Valley and Washington, D.C. The practice was selected as a 2013 "Intellectual Property Practice Group of the Year" by Law360.

King & Spalding's national appellate practice has established a reputation for successfully representing clients in major appeals in virtually every litigation forum, including before the U.S. Supreme Court, the federal and state appellate courts, government agencies, and national and international arbitration panels. Law360 selected King & Spalding's appellate group as a 2013 practice group of the year based on the significance, size, complexity and number of appellate matters it handled. The group has also been recognized by Chambers USA and Legal 500 as among the nation's best.

Steven Snyder to Discuss Cyber-Protection at Technology and Cloud Transactions Conference

Charlotte Intellectual Property partner Steven Snyder will be a featured panelist at the Law Seminars International's second annual Technology and Cloud Transactions conference on April 27 in Atlanta. The panel is entitled, "Getting Your House in Order Before Contracting: Data Asset Protection Plans to Avoid Security Breaches" and Snyder will discuss federal cyber-protection frameworks and requirements.

Kenneth Steinthal Named to Daily Journal's Top IP Attorneys of 2015

SAN FRANCISCO, Calif., May 5, 2015 — The Daily Journal has selected Kenneth Steinthal, a partner at King & Spalding, as one of California's leading intellectual property attorneys for 2015.

The Daily Journal's Top IP Attorneys annual ranking, published April 22, highlights the leading intellectual property attorneys in the state of California, recognizing "their ability to stay on the cutting edge of new developments in patent, copyright and trademark law," according to the publication's editors, who added: "The list demonstrates the impressive and diverse work done by California attorneys whose work advances the state's leadership in intellectual property law."

Steinthal was recognized, in particular, for his work on behalf of Pandora Media, Inc., in litigating against music performing rights organizations ASCAP and BMI. Steinthal and his team successfully challenged the efforts of those organizations (and their affiliated music publishers) to narrow the scope of the licenses available to Pandora and also obtained a very favorable-to-Pandora rate determination after trial for Pandora's performance of ASCAP works. In 2014, Steinthal also was selected by the American Antitrust Institute as a finalist for its Outstanding Antitrust Litigation Achievement in Private Law Practice award for his role as lead counsel in the Pandora-ASCAP litigation.

Steinthal has a high-profile international practice focusing on intellectual property rights matters arising from the distribution of audio and audiovisual content. He has litigated copyright infringement and rate-setting cases in both traditional and new media contexts. He also counsels clients on numerous copyright, music rights, DMCA safe harbor and other issues arising from his clients' content distribution activities.

King & Spalding Opens New Office in Tokyo

TOKYO, June 16, 2015 — King & Spalding will open an office in Tokyo, the firm's eighteenth office overall and tenth office outside the United States. The new Tokyo office, along with the firm's Singapore office, will anchor King & Spalding's market-leading energy practice throughout the Asia-Pacific region.

Joining King & Spalding as partners are Ashurst partners John McClenahan, Mark Davies, and Chris Bailey in Tokyo, and Rupert Lewi in Perth, who will form the core team and launch the firm's Tokyo office. Well-known in the Tokyo market, this highly-regarded group represents major Japan- and Korea-based actors in the energy and resources sector including export credit agencies and financial institutions, as well as some of Japan's largest trading houses, public natural gas companies and other blue chip project sponsors and participants. They have extensive experience supporting the development, financing and acquisition of, and resolution of disputes arising out of, major energy projects globally, including power generation facilities, gas pipeline infrastructure, floating production storage and offloading vessels, and LNG terminals.

"We are excited to build a new office around a top-tier team with deep roots in the Japanese legal marketplace and expertise in energy, projects, finance, construction and international arbitration," said Robert D. Hays, Jr., chairman of King & Spalding. "Given our momentum globally, strategic focus on energy, the growth of energy and related activity in Asia-Pacific, and the opportunity to launch with an internationally recognized group, Tokyo presents a real opportunity for us."

The Tokyo office, the firm's second in Asia, will focus on cross-border investment, project development, project finance, and global disputes work. It is expected to capitalize on the momentum of the firm's Singapore office where there are 10 resident partners – three focused on the power sector, three on oil and gas and LNG, and four on international arbitration. Earlier this year, the Singapore office recruited Richard Nelson, formerhead of the Southeast Asia energy practice at Herbert Smith Freehills, and Simon Cowled, a power projects partner from Skadden, Arps, Slate, Meagher & Flom. Chambers ranks several King & Spalding practices in Singapore noting its work in International Arbitration (Band 1) and Energy & Natural Resources (Band 1).

"The King & Spalding name is a calling card in the energy and international arbitration space in Asia," said McClenahan. "As a platform for growth, we see this as a great opportunity for each of us and we are excited about collaborating with our new colleagues across the firm."

Philip Weems, head of King & Spalding's energy practice, added "Our Tokyo presence enjoys a natural connection with the rest of the firm's energy practice. The new team will bolster what the firm has already achieved in the LNG, oil and gas, power and mining arenas, and our presence in Tokyo, an important hub of the world-wide energy market, further increases our global reach."

John McClenahan, who will serve as managing partner for King & Spalding's Tokyo office, has worked in Tokyo for over 20 years and played a lead role in the building of Ashurst's Japan/Korea practices. He specialises in banking and project finance and advises lenders, sponsors, project companies and contractors on major infrastructure projects, including in the power, petrochemicals and transportation sectors. He also advises clients on acquisition finance, structured finance transactions, cross-border acquisitions and joint ventures.

Rupert Lewi practices in the oil and gas, LNG and mining areas, with a focus on corporate and asset acquisitions and divestments, project structuring and project development work. He has counseled clients on leading LNG projects in Australia, Asia and the Middle East. Lewi, who previously worked in Tokyo for over 12 years, acts for a wide range of North Asian trading companies and gas and electricity utility companies, including in their overseas investments in Australia, the Asia-Pacific region and Africa.

Mark Davies has worked in Asia for more than a decade focusing on investment funds, project finance, asset finance and corporate finance transaction and M&A. He has gained considerable experience on a broad range of transactional matters across a number of key Asian jurisdictions.

Christopher Bailey is a highly experienced international arbitration practitioner and solicitor advocate who arrived in Tokyo in 2006 from an energy litigation background in London. He represents Japanese and Korean clients on their global disputes in the energy, resource, transport, infrastructure, financial service, media and IT sectors. His practice also extends to contentious regulatory, sanctions, compliance and investigations work. On the latter, Bailey has significant experience of major African and the Middle Eastern corruption investigations before regulators including the US Department of Justice and the UK Serious Fraud Office.

Legal 500 Names King & Spalding 2015 Firm of the Year for Supreme Court and Appellate

WASHINGTON, D.C., June 15, 2015 — Legal 500, in its annual awards, has named King & Spalding firm of the year for the Supreme Court and Appellate category for 2015.

King & Spalding's Supreme Court and Appellate practitioners are "highly respected," according to Legal 500, which also noted the contributions of partners Jeffrey Bucholtz, Daryl Joseffer and Ashley Parrish, all members of the firm's Appellate, Constitutional and Administrative Law Group.

Legal 500 bases its annual awards on the research and interviews that were conducted for its annual rankings, which were also released this month. For both the awards and rankings, Legal 500 researchers conduct thousands of interviews with attorneys and clients across the country.

King & Spalding's Washington, D.C.-based Appellate, Constitutional and Administrative Law Group has broad experience in complex appellate litigation at all levels of the state and federal court systems. The group's appellate lawyers are sought out for their strategic advice and counseling, persuasively written briefs, and superior oral advocacy skills. In 2014, King & Spalding's appellate team was selected as "Appellate Practice Group of the Year" by Law360.

Contacts

Thomas J. Gray	Holmes Hawkins	Steven Snyder	Christopher C. Carnaval
Editor / Partner	Practice Group Leader/Partner	Partner	Senior Associate
tgray@kslaw.com	hhawkins@kslaw.com	ssnyder@kslaw.com	ccarnaval@kslaw.com
+1 650 422 6723	+1 404 572 2443	+1 704 503 2630	+1 212 556 2154

Our Intellectual Property Practice Group

King & Spalding offers clients a full-service intellectual property (IP) practice that combines proven first-chair trial and business lawyers with true scientific specialists. The firm's Intellectual Property Practice Group consists of more than 90 IP professionals, including more than 70 lawyers and patent agents with technical degrees, located in our Atlanta, Austin, Charlotte, Houston, Moscow, New York, San Francisco, Silicon Valley and Washington, D.C., offices. The practice was selected as a 2013 "Intellectual Property Practice Group of the Year" by Law360.

King & Spalding has specialized expertise in Section 337 cases before the International Trade Commission. Unique among firms, we have leading practices in the three disciplines necessary in Section 337 cases: we combine our broad-based patent litigation experience and technical expertise, international trade expertise and expertise in the ITC's procedures, and a strong governmental relations group. King & Spalding has been involved in some of the largest, most complex and precedent-setting Section 337 cases.

About King & Spalding

Celebrating more than 125 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 800 lawyers in 17 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients. More information is available at www.kslaw.com.