

Traversing the Breach: Why You Need to Prepare for Data Breaches and How to Do It

“At every board meeting, whether it’s monthly, whether it’s quarterly, cybersecurity should be on [the agenda]. If not, you’re going to wind up in a situation where you’re having an emergency board meeting to discuss something that has gone wrong. You have to have a plan. You should have general counsel, public relations, communications, the IT people, the security people—all of them need to have a structure in place to be able to deal with something like this.” —Howard Schmidt, former White House Cybersecurity Czar, *Wall Street Journal*, Feb. 9, 2015. (See <http://www.wsj.com/articles/what-business-and-the-feds-should-do-about-cybersecurity-1423540851>.)

For several years, the common business refrain has been that “every company is a tech company,” as brick-and-mortar businesses turn to technology to distinguish themselves and enhance efficiency, intelligence, and customer experience. The corollary, of course, is that every company now also is a data company. In a world where transactions are conducted digitally and corporate strategy is driven by sophisticated analytics, data is fast becoming a company’s greatest asset. Almost everything a company cares about is increasingly stored in digital banks.

Unfortunately, as the recent string of high-profile security breaches—Target, Sony, Anthem—has made

(continued on page 2)

INSIDE

Direct Purchasers and End Payors Accuse Brand Pharma of Delaying Generic Entry
Page 5

Practice Area Updates:

Patent Litigation Update
Page 6


Entertainment Litigation Update
Page 7

International Arbitration Update
Page 7

Asia-Pacific Litigation Update
Page 8

Court Stays Lawsuit Against IBM Pending Resolution of Related International Arbitration Involving an IBM Subsidiary and Other Victories
Page 10


The National Law Journal Names Quinn Emanuel to Its 2014 “Appellate Hot List”

The National Law Journal has once again named Quinn Emanuel to its “Appellate Hot List,” marking the fourth time the firm has received this recognition in the past five years. The firm was selected as a result of several major appellate victories, including a notable Federal Circuit win for Google reversing a \$30.5 million verdict, a landmark Second Circuit decision on behalf of the Federal Housing Finance Agency that enabled more than \$20 billion in settlements, and a major Federal Circuit win for Samsung against Apple in the ongoing patent litigation between the two smartphone giants that once again prevented Apple from obtaining injunctive relief against Samsung. In other appellate news for the firm, In 2014, Kathleen Sullivan, Chair of the firm’s Appellate Practice, was honored by election to the American Academy of Appellate Lawyers, a prestigious group limited only to the top appellate lawyers in the U.S. 

Quinn Emanuel Adds London Based Competition Star Boris Bronfentrinker to Its Global Competition Group

page 9

Karl Stern Joins Houston Office

Karl Stern has joined the Houston office as a partner and head of the office’s civil litigation practice. Mr. Stern joins the firm from Vinson & Elkins LLP, where he served in various leadership positions, including Managing Partner of the Houston office and Firmwide Head of Litigation. Mr. Stern’s practice focuses on complex business disputes of all kinds, including antitrust, securities, M&A, fiduciary litigation, and complex disputes in the energy industry. He has over 30 years of extensive experience trying cases to juries, courts, and arbitrators within state and federal courts throughout the U.S. and before domestic and international arbitral tribunals. Mr. Stern has been repeatedly recognized as a leading individual by a wide range of legal publications, including *The Best Lawyers in America*, *The Legal 500 USA*, *Euromoney’s Benchmark Litigation*, and *Global Arbitration Review*. 

clear, the increasing value of data has been met with rising risk. As James Comey, director of the FBI, observed in a recent interview, “Cybercrime is becoming everything in crime. . . . Because people have connected their entire lives to the Internet, that’s where those who want to steal money or hurt kids or defraud go.” (See <http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/>.) Moreover, data security has become as much a legal issue as a technological one, as companies face a bewildering array of federal, state, and international laws and regulations governing cybersecurity, privacy, and breaches. In this quickly evolving climate, it is imperative that companies closely examine their breach preparedness from both a security and legal standpoint. The hours after a breach may well determine how a company fares.

Companies Face an Increasing Risk of Data Breach

The proliferation of security breaches poses an enormous threat to customers, and to the reputation and bottom line of compromised companies. In 2014, Ponemon found that 43 percent of U.S. companies had experienced a data breach within the last year, up from 33 percent in 2013. Moreover, even before the most recent breaches, it found data breaches were costing U.S. companies an average of \$5.9 million, or an average of \$201 for each compromised record. A brief review of some of the most prominent recent data breaches illuminates the breadth of industries affected by breaches, as well as the scope of potential damage.

- On February 3, Anthem, the nation’s second-largest health insurer, announced a data breach that had exposed the personal information, including Social Security numbers, of 80 million customers and employees. Anthem’s breach is the latest and largest in a series of data security issues affecting the health industry. In August 2014, Community Health Systems announced a data breach that had exposed 4.5 million patient records. Experian forecasts that data breaches may cost the healthcare industry as much as \$5.6 billion annually.
- In perhaps the most notorious recent data breach, in November 2014, hackers obtained and released terabytes of internal data at Sony Pictures Entertainment, including embarrassing corporate documents and Social Security data for 47,000 Sony employees. In addition, all data on many Sony servers reportedly was destroyed. The breach is estimated to have caused Sony \$70-\$80 million in direct costs, as well as potentially more than \$100 million in indirect costs from related loss of business. On February 4, Sony Pictures’ co-chairman resigned, largely due to fallout from the

breach.

- In September 2014, Home Depot revealed that a data breach had exposed 56 million customer debit and credit card accounts, then announced shortly afterward that 54 million customer e-mail addresses also had been compromised. In its SEC filing for the third quarter of 2014, Home Depot disclosed that it had recorded \$43 million in expenses arising from the breach.
- In August 2014, JPMorgan Chase disclosed that hackers had been siphoning data from its computer network for months, exposing contact information for 76 million households and 7 million small businesses. Subsequently, the bank announced that it would spend \$250 million annually to implement new security initiatives and protect itself from future cyberattacks.
- In one of the largest breaches in recent memory, in December 2013, Target disclosed that hackers had stolen names, credit card data, e-mail addresses and phone numbers for up to 110 million users. Following the announcement, Target’s profits plunged by 40 percent. In February, it was reported that losses associated with the breach had reached approximately \$200 million.

As the diversity of businesses affected—including healthcare, entertainment, financial and retail companies—demonstrates, data security is a critical issue not only for Internet businesses, but for all companies in all industries. As new mobile payment technologies emerge and companies continue to migrate data to BYOD programs and cloud-based systems, the risk of data breach is expected to continue to increase in 2015, heightening the need for companies to closely examine their own networks and data for security issues.

Companies Are Subject to Increasing Legal Risks and Obligations Relating to Data Security

Existing Legal Landscape. Companies that have experienced data breaches not only have suffered from losses in good will, customer attrition and technological costs, but also legal liability. The current legal landscape governing data privacy comprises a sprawling patchwork of state, federal and international laws, and class action lawyers, as well as state, federal and global regulators are becoming increasingly vigilant and aggressive. Following a data breach, a company can find itself under legal fire from multiple angles.

At the federal level, the Federal Trade Commission, the Securities Exchange Commission, and other regulators have been very forward-leaning. As part of its consumer protection duties, the FTC has actively investigated companies’ data privacy and collection

policies, levying monetary penalties and requiring companies to implement improved security policies subject to independent monitoring. It also has brought actions under the Fair Credit Reporting Act and the Gramm-Leach Bliley Act following breaches exposing consumers' credit histories and financial data. The SEC's Division of Corporation Finance has issued guidance regarding public reporting requirements for cybersecurity incidents, and Commissioner Luis Aguilar has confirmed that the SEC will hold boards of directors accountable for their companies' cybersecurity risk management policies. Meanwhile, the Financial Industry Regulatory Authority and the SEC's Office of Compliance Inspections and Examinations have begun examining the cybersecurity preparedness of regulated entities, with both bodies releasing reports of their findings and suggested best practices at the beginning of February.

At the state level, state attorneys general have taken an increasingly active role in investigating data breaches and enforcing privacy protections, with multi-state investigations currently underway regarding the breaches at Target, Home Depot and JPMorgan Chase. In these cases, states are investigating not only whether proper safeguards of consumer data were in place, but also whether after discovering their breaches, the companies properly notified affected customers. As 47 states have enacted some form of security breach notification statute over the last decade, each with varying timing and threshold requirements, compliance with notification statutes has presented serious issues for companies with widespread consumer bases. These issues are compounded for international companies, as notification statutes in other countries—including in the European Union—impose even more stringent disclosure requirements than those in the United States.

Finally, every prominent data breach has prompted a flood of consumer class action lawsuits, usually including a combination of negligence, contract, state consumer protection and federal privacy claims. Multiple lawsuits were filed against Anthem and Sony within hours of breach disclosures, and Home Depot disclosed that it has been named in at least 44 consumer lawsuits. Historically, companies have had success defeating consumer claims by challenging standing, arguing that without concrete allegations of actual identity theft, plaintiffs could not demonstrate classwide harm from the mere exposure of their data. Recently, however, courts have shown an increasing willingness to allow such claims to proceed. In September 2014, the Northern District of California permitted a data-breach class action to proceed against Adobe, holding that a "credible threat of real and immediate harm" in

the future was sufficient to confer Article III standing on the class. *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-cv-051126, 2014 WL 4379916, at *6-*9 (N.D. Cal. Sept. 4, 2014).

New Legislative Developments. As data security continues to dominate the national conversation, federal and state lawmakers are rushing to update the existing body of privacy laws. The White House has made data privacy a major priority this term, proposing legislation that would reconcile inconsistent state notification statutes by creating a uniform federal standard for data breach notification. At the same time, California, New York and other states are continuing to amend and broaden their own notification statutes to cover additional entities and forms of data. In the financial sector, state regulators also issuing their own guidelines, and New York's Department of Financial Services recently announced that it would start conducting its own preparedness assessments of banks and insurers. As new laws are proposed and go into effect, it is critical for a company to understand the legal obligations that may apply in each area it does business.

Companies Must Take Proactive Steps to Mitigate Exposure and Ensure Legal Compliance

It goes without saying that companies should take steps to safeguard customer privacy and to minimize the potential for a data breach. However, given the continued rise in frequency and sophistication of cybercrime, as well as the growing attention to notification requirements, companies must make it an equal priority to prepare themselves to respond when breaches inevitably occur. It is not only the smart thing to do, it is becoming the standard of care.

Given the complicated technical and legal issues involved, data breach preparedness can be a source of anxiety to companies. In Ponemon's 2014 survey, 73 percent of companies reported that they had data breach response plans and teams in place, but only 30 percent believed that their plans were effective. Below are a few high-level guidelines that a company should follow when assessing its readiness for a breach.

Conduct a Readiness Audit. At a minimum, a company should assess its legal compliance and infrastructural ability to respond to an attempted breach by conducting a readiness audit. As part of this audit, a company should:

Map data and backups. Because the nature of data drives both the level of security and the legal obligations that flow after a breach, a company needs to know what data it has and where it is located. Put simply: the more important data is, the better the security should be. Moreover, in the case of a breach, knowing what was

taken and where it was collected/located will determine a number of legal obligations. Finally, a company must have a realistic way to restore lost data or take parts of its system offline without causing more problems. Backups need to be done in a way that makes this possible.

Perform a network security assessment. Once a system map is in place, regular “penetration testing” must be conducted to identify potential system vulnerabilities. This includes subjecting company employees to phishing tests so that passwords are not inappropriately disclosed. Education is a must, and all employees should be aware of how to observe security precautions and avoid allowing unauthorized access.

Review insurance policies and contracts. With the rash of security breaches, insurance policies are now available to cover costs associated with data breaches, including notification, public relations, and resulting legal and liability expenses. Some policies even cover the costs of assessing the company’s preparedness for a data breach.

Monitor the legal landscape. In view of the ever-changing legal landscape, a company should engage legal counsel to identify and assess compliance with the universe of applicable state, federal and international regulations. Because even simple business decisions (e.g., requesting a physical address or changing the way data records are stored) can trigger new obligations in different territories, counsel must be consulted on an continual basis so that companies are accurately informed about their ongoing risks and obligations.

Maintain law enforcement contacts. In the event of a significant breach, law enforcement involvement will be necessary to identify and bring to justice the intruders. A company should establish contact with the state and federal law enforcement individuals that have jurisdiction in its industry or geographical area. In the event of a breach, legal counsel should manage any communications with law enforcement.

Prepare a Cyber Incident Response Plan. In addition to conducting a readiness audit, a company must have a comprehensive cyber incident response plan to minimize potential losses, keep customers informed on a timely basis, and avoid further legal liability in the event of a breach. Any response plan must assume that all internal systems are compromised. In developing this plan, a company should:

Prepare a legal response and notification strategy. A company must have a legal response and notification plan that complies with all applicable notification provisions. Legal counsel should be heavily involved both in drafting the plan and advising during its implementation as to when and where different notification duties may be triggered.

Prepare a communication strategy. A company


should have not only an external communication strategy for satisfying notification requirements and customer expectations and needs, but also an internal communication strategy. All parties must be mindful of the risk that non-privileged communications may be subject to discovery in the event of a lawsuit or investigation. Employees or call center representatives should have clear guidance for all communications concerning a breach.

Prepare a forensic and technical response strategy. A company should identify all data that must be preserved and collected in the event of a breach. This data will not only be used for troubleshooting, monitoring, and recovery, but also as a record that will be used by regulators, lawyers and law enforcement after a breach. Forensic experts should be engaged to collect and examine the data as internal IT teams focus on restoring systems. To maximize work product and privilege protection, lawyers should hire and direct the forensic experts.

Designate response officials. A company should identify key employees who are knowledgeable of each critical area and who will be responsible for executing the response plan. At a minimum, legal counsel, company executives, communications, IT, and HR representatives (if employee actions or information are at issue) should be included.

Distribute call lists and written response plans. Once a detailed response plan has been prepared, it should be memorialized and distributed outside of the company’s computer systems to all relevant individuals. This should include a laminated call list of all designated response officials so that the plan can be put into effect immediately.

A cyber incident response plan necessarily is a sensitive undertaking, as a company must investigate and repair any breaches while simultaneously keeping customers informed, preserving evidence and cooperating with authorities who may be evaluating the company’s security policies and response procedures in real time. It is critical to engage legal counsel not only when preparing the plan but also while executing it, to identify and navigate all potential legal ramifications and to protect attorney-client and work-product privileges.

Quinn Emanuel has a team of lawyers with the experience, knowledge, and relationships to help your company navigate the thicket of issues that accompany a data security incident. In addition, our international presence means Quinn is poised to act on a moment’s notice and get in front of any legal issues, no matter where the incident occurs. 

Direct Purchasers and End Payors Accuse Brand Pharma of Delaying Generic Entry

Americans want access to inexpensive pharmaceutical drugs. This demand must be balanced with the fact that brand-name, innovator pharmaceutical companies typically invest tremendous resources to research and develop new drugs, bring them to market and obtain patent protection for their inventions. To address these often competing interests, Congress passed the Drug Price Competition and Patent Term Restoration Act of 1984, Pub. L. No. 98-417, also known as the “Hatch-Waxman Act,” which created a regulatory framework that seeks to balance an incentive to innovate with public access to inexpensive generic drugs.

Specifically, the Hatch-Waxman Act provides generic pharmaceutical companies with a simplified process to compete with innovator pharmaceutical companies through the filing of an Abbreviated New Drug Application (“ANDA”), in exchange for certain exclusivity periods for the innovator. The generic companies are permitted to rely on safety and efficacy studies conducted by the innovator if the generic company can demonstrate that its drug is “bioequivalent” to the approved innovator drug product. 21 U.S.C. § 355(j)(2)(A). ANDA filers also generally seek to have their product deemed “AB-rated,” which means their drug is pharmaceutically equivalent to the brand-name drug. Without this rating, a pharmacy may not automatically substitute a generic drug for a brand-name drug.

However, the ANDA process does not always work quickly, and direct purchasers and end payors for pharmaceuticals have recently asserted several class action lawsuits against innovator drug companies alleging that certain of the innovators’ actions are subject to antitrust liability because they result in delayed generic market entry. Innovators have responded to these actions by moving to dismiss, seeking to halt what they perceive as baseless antitrust actions before they even start. This scenario played out recently in *In re Suboxone (Buprenorphine Hydrochloride and Naloxone) Antitrust Litigation*, MDL No. 2445.

There, the direct purchasers and end payors (the “Plaintiffs”) alleged that Reckitt Benckiser, Inc. (“Reckitt”) violated the Sherman Act and several state laws by engaging in three acts to delay the entry of a generic version of its Suboxone product: (1) a “product hopping” scheme; (2) the filing of a “sham” Citizen Petition; and (3) refusing to give favorable terms in a negotiation with the generics (the “duty to deal” claim). On December 3, 2014, the District Court for the Eastern District of Pennsylvania issued an Opinion permitting discovery to go forward on the “product

hopping” and “sham” Citizen Petition claims, but dismissing the Plaintiffs’ duty to deal claim. *Id.*, Slip Op. (D.I. 97) (E.D. Pa. Dec. 3, 2014). Reckitt has moved for reconsideration of the Court’s denial on the “product hopping” and “sham” Citizen Petition claims.

Product Hopping

The Plaintiffs alleged that Reckitt engaged in a product hopping scheme by switching from a tablet to a film version of Suboxone. *Id.* at 1. Reckitt pulled its tablets from the market in favor of the film, asserting that the tablet presented safety concerns regarding accidental pediatric exposure, which the film solved. *Id.* at 5. The Plaintiffs characterized Reckitt’s safety concerns as “a fraudulent sales and marketing campaign against the tablet for the purpose of diverting sales from the tablet.” *Id.* The Plaintiffs complained that Reckitt’s switch to a Suboxone film would delay generic entry because: (1) the patent for the Suboxone film extends until September 2023; and (2) generic Suboxone tablets cannot be AB-rated to the film form and, therefore, a pharmacist cannot automatically substitute the generic tablets for a prescription to the brand-name film. *Id.* The Court found that the “facts presented sufficiently allege that the disparagement of the Suboxone tablets took place alongside ‘coercive measures’” and, thus, denied Reckitt’s motion to dismiss the “product hopping” claims. *Id.* at 18-22.

“Sham” Citizen Petition

Reckitt’s safety concerns regarding the Suboxone tablets also led it to file a Citizen Petition with the FDA, asking the FDA not to approve generic versions of the Suboxone tablet until the FDA made several safety conclusions regarding the pending ANDAs seeking approval to market generic tablets. *Id.* at 7-8. The Plaintiffs alleged the Petition was a sham because the FDA did not have the authority to enforce any of Reckitt’s safety requests and because Reckitt was allegedly taking actions inconsistent with what it asked for in the Citizen Petition. *Id.* at 8-9. The Plaintiffs also noted that the ANDAs were approved immediately after the Citizen Petition was denied. *Id.* at 9. The Court agreed with the Plaintiffs, finding that they plausibly pleaded that Reckitt used the Citizen Petition to interfere with the ANDA approvals, and “plausibly pleaded that the Petition was objectively baseless in that no reasonable litigant could have realistically expected success on the merits.” *Id.* at 31-32. Thus, the Court denied Reckitt’s motion to dismiss these claims.

NOTED WITH INTEREST (cont.)

Duty to Deal

The FDA approved a Risk Evaluation and Mitigation Strategy, or “REMS,” for Suboxone tablets based on the concern of pediatric exposure. *Id.* at 6. The FDA, then, ordered the ANDA filers to collaborate with Reckitt on a Single Shared REMS (“SSRS”) that would control the distribution of both generic and branded Suboxone products. But the Plaintiffs alleged, pursuant to 21 U.S.C. § 355-1(f)(8), that Reckitt was attempting to use its REMS “to block or delay approval of” their ANDAs, and unlawfully maintain monopoly power. *Id.* at 27. Specifically, they alleged that Reckitt refused to attend SSRS meetings, insisted on conditions the generic manufacturers found unreasonable, and refused to disclose confidential information from its own REMS. *Id.* at 7.

The district court held that 21 U.S.C. § 355-1(f)(8) does not create an antitrust duty to deal in the context of negotiations for a SSRS, especially where the

branded company’s REMS does not prevent generics from obtaining samples of the brand-name drug for bioequivalence testing. The Court further held that, to the extent that § 355-1(f)(8) does create a duty to deal, the statute also “provides for increased FDA oversight and diminishes the need for antitrust scrutiny.” *Id.* at 29. Thus, the Court granted Reckitt’s motion to dismiss the duty to deal claims.

This case is one of several recent filings where end purchasers and payors have raised these and similar issues. This is the first opinion to issue, and Reckitt’s motion to reconsider remains pending, so the ruling does not necessarily indicate what this and other courts will do in the future. That said, there is a growing trend indicating that end purchasers and payors will continue bringing these types of claims against innovator pharmaceutical companies. Those companies should monitor the developing case law and be advised of the potential pitfalls it may raise. [Q](#)

PRACTICE AREA NOTES

Patent Litigation Update

Supreme Court to Review Good Faith Defense to Patent Inducement Claims. Last month in *Commil USA, LLC v. Cisco Systems, Inc.*, 720 F.3d 1361 (Fed. Cir. 2013), *cert. granted in part*, No. 13-896, 2014 WL 318394 (U.S. Dec. 5, 2014), the Supreme Court granted review of the Federal Circuit’s decision in *Commil USA, LLC v. Cisco Sys.*, 720 F.3d 1361 (Fed. Cir. 2013). The Court will address whether the Federal Circuit erred in holding that a defendant’s belief that a patent is invalid is a defense to induced infringement under § 271(b). This is the latest in a line of decisions originating from *DSU Medical Corp. v. JMS Co.*, 471 F.3d 1293 (Fed. Cir. 2006). In that case, the Federal Circuit resolved a split in its precedent over the level of intent required to establish active inducement in patent infringement cases. Prior to *DSU*, the Federal Circuit applied both a general and specific intent standard. Under its general intent standard, the Court required that a defendant intend to engage in acts (such as selling a potentially infringing component of an infringing product) that ultimately resulted in direct infringement, apparently without regard to whether the defendant knew its acts would result in direct infringement. Under its specific intent standard, the Court required an additional showing that the defendant actually knew or should have known that its acts would result in direct infringement. In *DSU*, the

Federal Circuit decided, *en banc*, to apply the specific intent standard. The Federal Circuit also held that an accused infringer’s good faith belief of non-infringement can be used to establish a lack of intent. In *DSU*, an opinion of counsel was successfully used to establish that an accused infringer had a good faith belief that the accused products did not infringe, and could therefore not be held liable for inducement.

In *Commil*, the Federal Circuit expanded the boundaries of this “good faith belief” to include invalidity. Specifically, the Federal Circuit found that a good faith belief that the asserted patent was invalid (for example, by relying on an opinion of counsel) could provide a basis for negating intent. Reasoning that “one cannot infringe an invalid patent,” the majority concluded that one could have knowledge of the existence of a patent and induce others to infringe it, yet still lack the intent for induced infringement through a “good-faith belief that the patent is not valid.” The Federal Circuit made clear that a finding of a good faith belief of invalidity does not preclude a finding of induced infringement, but is evidence that should be considered by the fact-finder.

Following a denial by the Federal Circuit to reconsider its decision, *Commil*, the patentee, filed a petition for writ of certiorari in January 2014. Last month, the U.S. Supreme Court granted certiorari on the first issue presented in *Commil*’s petition: whether the Federal Circuit erred in holding that a defendant’s belief that a

patent is invalid is a defense to induced infringement under § 271(b). In its petition, Commil argued that the decision created a new good faith defense that would “dramatically weaken the Patent Act’s provision of liability for inducing infringement.” Commil also protested that the decision would dramatically increase the costs of litigation and make it too easy for defendants to escape patent infringement claims.

Cisco, the defendant, countered that there is no principled distinction between a good faith belief of non-infringement and a good faith belief of invalidity. Because a good faith belief of non-infringement negates intent under *DSU Medical Corp. v. JMS Co.*, the same principle should apply to a good faith belief of invalidity.

The solicitor general, after being asked by the Supreme Court to weigh in on Commil’s petition, filed an amicus brief in October 2014 agreeing with Commil that the opinion warranted review because “that holding is inconsistent with the Patent Act’s text and structure, and it may undermine Section 271(b)’s efficacy as a means of deterring and remedying infringement.”

Entertainment Litigation Update

United States v. Dish Network LLC: *The Increasing Risks of Liability for Authorized Dealers.* An Illinois district court issued an important ruling under the Telephone Consumer Protection Act and other telecommunications laws in December, adopting an inclusive view of companies’ liability for non-compliant telemarketing by affiliated third parties. The Court granted partial summary judgment to the government on claims that Dish Network LLC (“Dish”) was liable for the acts of its authorized dealers. The case is an illustration of the increasing risk to companies that use purported independent contractors in an attempt to shield themselves from liability.

The federal government and four states alleged that Dish Network—on its own, through telemarketing vendors, and importantly through authorized retailers who conduct telemarketing—caused tens of millions of calls to be made in violation of the Telephone Consumer Protection Act, Telemarketing Consumer Fraud and Abuse Prevention Act, FCC and FTC Rules and state statutes. The prohibited conduct, primarily, was calling people on the National Do Not Call Registry.

Dish Network generally acknowledged responsibility for the conduct of telemarketing vendors as its agents, but contested vicarious liability for the telemarketing activities of authorized retailers, which it argued were independent contractors and not agents as a matter of law. However, the court disagreed in three respects, highlighting the evolving ways in which a company may become liable for the conduct of third party business

affiliates, including independent contractors.

First, during the litigation, the parties petitioned the FCC to interpret a rule imposing liability on the seller for calls made to Do Not Call registrants on its behalf. The FCC determined that sellers could be liable for improper calls under federal common law principles of agency that not only include formal agency but also a broad range of other agency theories such as apparent authority and ratification. The court reviewed Dish’s retailer contracts—which defined retailers as independent contractors—and concluded that factors like Dish’s ability to make and change retailer program rules suggested agency.

Second, the Telemarketing Sales Rule (“TSR”) prohibits giving substantial assistance to a telemarketer where one knows or consciously avoids knowing that the telemarketer is violating the TSR. Concerning one authorized retailer, the court found Dish had responded promptly when it learned of TSR violations and could not be liable. Concerning another, however, the court found Dish had indications that the retailer was violating the TSR and continued to do business with it.

Finally, the TSR imposes liability where a seller “causes” a telemarketer to call individuals on the Do Not Call Registry to sell the sellers’ products. The FTC’s interpretation of “causes,” to which the court deferred, requires only that the seller retained the retailer, the seller authorized the retailer to sell its products, and the retailer made prohibited calls. As Dish had permitted certain retailers to sell Dish products through telemarketing, the court granted summary judgment against Dish on liability, finding Dish liable for over 57 million improper calls. The number of authorized dealers, compared to the number of Dish’s vendor agents who made those calls was a significant consideration: Dish and its vendor agents made 5.2 million calls; Dish’s authorized retailers made the remaining 51.8 million.

The case name is *U.S., et al. v. Dish Network LLC*, case number 3:09-cv-03073 in the U.S. District Court for the Central District of Illinois.

International Arbitration Update

Accounting for “Country-Risk” in Assessing Damages in Investor-State Arbitration: *Gold Reserve Inc. v. Bolivarian Republic of Venezuela, ICSID Case No. ARB(AF)/09/01, Award (Sept. 22, 2014).* The careful treatment of the parties’ valuation submissions in this Award provides valuable insight into the approach to valuation of natural resource assets in the context of investor-state arbitration.

An arbitral tribunal under the auspices of the International Centre for Settlement of Investment Disputes (“ICSID”) recently awarded the claimant Canadian mining company over U.S. \$713 million

in damages for violations of the Canada-Venezuela bilateral investment treaty (the “Agreement Between the Government of Canada and the Government of the Republic of Venezuela for the Promotion and Protection of Investments”, dated July 1, 1996 and in force January 28, 1998, or the “BIT”), for wrongful termination of its mining concessions, as well as pre- and post-award interest and a portion of its costs.

Gold Reserve owned two mining concessions in Venezuela conferring upon it the right to extract gold, copper and molybdenum, with “mineral reserves... estimated to be 9.087 million ounces of gold and 985 million pounds of copper”. Gold Reserve had invested approximately U.S. \$300 million in developing the project, but it had not yet commenced commercial mining when Venezuela wrongly rejected a request to extend one concession at the expiry of its initial term, and purported to terminate both.

Gold Reserve commenced proceedings for breach of the BIT under the ICSID Additional Facility rules. The Tribunal found Venezuela to be liable for breach of the BIT by denying Gold Reserve’s “due process rights by failing to initiate a specific administrative procedure to revoke the extensions” of Gold Reserve’s concessions.

The Tribunal’s valuation of Gold Reserve’s investment relied on the principles of public international law established by the Permanent Court of International Justice in the *Chorzów Factory* case, namely that “reparation should as far as possible eliminate the consequences of the illegal act and re-establish the situation which would, in all probability, have existed if that act had not been committed.” To calculate the damages required to achieve this effect, the Tribunal adopted a discounted cash flow “DCF” analysis to determine the market value of the concessions at the date of the treaty breach. The Tribunal’s approach to the country risk premium applicable in this analysis is particularly noteworthy.

Although both parties’ experts agreed that the discount rate to be applied should reflect the claimant’s weighted average cost of capital “WACC”, the parties disagreed over several elements of its calculation. As the Tribunal noted, “the largest discrepancy concerned the country risk premium applied as part of the cost of equity.” Gold Reserve asserted a country risk premium of 1.5% and Venezuela advanced rates between 6.7% and 16.4%. The discrepancy was due in part to Venezuela’s financial expert applying a risk premium that “took account of Venezuela’s policies at the time, including the President’s policy of ousting North American companies from the mining sector, thus increasing the risk significantly.”

The Tribunal agreed with Gold Reserve’s expert, who contended that it “was not appropriate to increase the

country risk premium to reflect the market’s perception that a state might have a propensity to expropriate investments in breach of BIT obligations.” Although finding the risk premium advanced by Gold Reserve’s expert too low (because it posited a “but for” scenario in which the host State would not misuse its sovereign power), the Tribunal found that Venezuela’s risk premium was too high because it “include[d] some element reflective of the State policy to nationalise investments”. The Tribunal ultimately adopted a country risk premium of 4%, explaining that this rate was reasonable “but has not been over-inflated on account of expropriation risks”.

This analysis may be contrasted with another recent ICSID award, in *Exxon Mobil v. Bolivarian Republic of Venezuela*, ICSID Case No. ARB/07/27, Award, (Oct. 9, 2014), also stemming from the late President Chávez’s nationalization policies. In that case, the Tribunal stated that it “...considers that the confiscation risk remains part of the country risk and must be taken into account in the determination of the discount rate.” For some commentators the *Exxon Mobil* Tribunal’s reasoning might inadvertently encourage a host State to create a higher perception of expropriation risk in the markets, by political acts or statements, prior to expropriating a strategic asset in the hope of lowering its exposure on damages in the event that it is later sued.

Asia-Pacific Litigation Update

Injunctive Relief for SEPs Limited in Japan. Japan appears to be limiting injunctive and exclusionary relief for holders of Standard Essential Patents (SEPs) encumbered by Fair, Reasonable and Non-Discriminatory (FRAND) licensing terms. On May 16, 2014, Japan’s Grand Panel of the IP High Court issued a decision holding that a holder of FRAND encumbered SEPs was not entitled to a preliminary injunction but was prima facie entitled to damages.

Injunctions are commonly granted in Japan as a matter of law following a finding of patent infringement. On February 28, 2013, however, after holding that certain electronic devices infringed FRAND-encumbered SEPs, the Tokyo District Court dismissed the petition for a preliminary injunction. (Case 38969 (wa), 2011; Case 22027 (yo), 2011; and Case 22098 (yo), 2011). The Tokyo District court held that the patent owner was not entitled to injunctive relief as well as damages because its misconduct during licensing negotiations constituted an abuse of rights. The court ruled that, as a FRAND-encumbered SEP holder, the patentee had violated its duty to negotiate in good faith. This was the first time that a Japanese court used the abuse of rights doctrine to deny an SEP holder’s right to seek damages and injunctive

relief. The patent owner appealed the decision.

On May 16, 2014, the Grand Panel of the IP High Court upheld the Tokyo District Court's decision dismissing the petition for a preliminary injunction but decided differently with respect to damages. (Case 10043 (ne), 2013; Case 10007 (ra), 2013; and Case 10008 (ra), 2013). The IP High Court held that the SEP holder was *prima facie* entitled to damages for patent infringement. However, the court found that the patent holder could not seek damages or relief in excess of any FRAND license fee because such damages or relief would be an abuse of rights.

Before issuing its decision, the IP High Court sought and received public comment as to whether injunctions and damages should be restricted for FRAND-encumbered SEP holders. According to expert commentators, the court's request for public comment was without precedent or basis in the Japan Civil Procedure Code. The 58 public comments received by the IP High Court is another aspect that makes this case extraordinary and significant for patent litigation practice going forward in Japan.

Trading Down Under. Australia has traditionally been an outward facing nation. The combination of a small population on a large continent has led to an export driven economy, and as such, Australia has placed great emphasis on trade arrangements. These arrangements were greatly augmented last year by a raft of trade agreements concluded with three of Australia's top four trading partners.

China-Australia FTA: China is Australia's largest two-way trading partner. Negotiations for the FTA concluded in November 2014, and the parties are now working towards signature.

Japan-Australia EPA: Japan is Australia's second largest two-way trading partner. The Economic Partnership Agreement entered into force on January 15, 2015.


Korea-Australia FTA: Korea is Australia's fourth largest

two-way trading partner. The FTA entered into force in December 2014.

These agreements are important in their own right. Quite apart from Australia being one of only a handful of western countries to negotiate a FTA with China, Australia has now concluded agreements with countries accounting for more than 60% of its bilateral trade.


However, the investment provisions in these agreements are of particular interest. This is because they represent a major shift in the Australian Government's position. In 2011, Philip Morris brought a claim against Australia under the Hong Kong-Australia Bilateral Investment Treaty. This claim arose from Australian legislation mandating that cigarettes only be sold in plain packages. As a result of Philip Morris' claim, the Australian Government publicly announced that it was modifying its negotiating stance so that future investment and trade agreements would not contain clauses permitting investors to bring claims directly against host states ('ISDS Clauses').

That position has changed. The Korea-Australia FTA includes an ISDS Clause. Likewise, although the negotiated text of the China-Australia FTA has not been released, it is also understood to contain an ISDS Clause. The Japan-Australia EPA did not contain an ISDS Clause; but the parties agreed to review that position if Australia subsequently agrees to an ISDS Clause with another country—as it has done with China.

Australia seems to be now firmly back on the investor-state arbitration bandwagon. Given the concerns many companies have about investing in China, it seems likely that some companies will structure their investments in China through Australia, and that the ISDS Clause in the China FTA will be put to use. Australia's trade agreements may well have an oversized impact on investment arbitration in the region. Close attention will now be paid to the near-final negotiations of the Trans-Pacific Partnership. 

Quinn Emanuel Adds London Based Competition Star Boris Bronfentrinker to Its Global Competition Group

Boris Bronfentrinker, a specialist in antitrust and competition law, has joined Quinn Emanuel as a partner based in the firm's London office. Mr. Bronfentrinker also has extensive experience with general commercial disputes and managing internal investigations. He was formerly a partner at Hausfeld LLP and before that, spent seven years as a member of Freshfields Bruckhaus Deringer's competition practice, primarily representing defendants. He brings to the firm a unique perspective, having significant experience in representing both

claimants and defendants in competition litigation. Mr. Bronfentrinker has represented clients in both the English High Court and the Competition Appeal Tribunal, as well as coordinating competition litigation claims in other jurisdictions. He also has experience with general commercial disputes and managing internal investigations. Mr. Bronfentrinker has degrees in both Law (*first class honors*) and Economics from the University of Sydney as well as a postgraduate degree in EC Competition Law from King's College, London. 

VICTORIES

Court Stays Lawsuit Against IBM Pending Resolution of Related International Arbitration Involving an IBM Subsidiary

On November 14, 2014, the U.S. District Court for the Southern District of New York stayed an action filed against International Business Machines Corporation (“IBM”) by Iusacell, S.A. de C.V. (“Iusacell”) on the ground that the action involved common issues with those to be determined in an International Chamber of Commerce arbitration now pending between Iusacell and IBM’s Mexican subsidiary, IBM de México, Comercialización y Servicios, S. de R.L. de C.V. (“IBM México”). The Court also declined Iusacell’s bid to take discovery while the stay is pending.

IBM México commenced an arbitration against Iusacell in Mexico City pursuant to the mandatory arbitration provision in the parties’ Master Services Agreement (“MSA”), and Iusacell counterclaimed. While the arbitration was pending, Iusacell filed a related action in federal court in New York against IBM, which was not a party to the MSA, not a signatory to an arbitration agreement, and not a party to the arbitration. Iusacell’s New York allegations against IBM mirrored those it advanced in the arbitration.

Quinn Emanuel represented IBM and moved to stay the New York action, relying on the New York court’s inherent, discretionary authority to stay an action involving a nonparty to a pending arbitration on the ground that resolution of the issues in the arbitration may be determinative of issues in the case. Rejecting Iusacell’s argument that the propriety of a stay of the New York action should be determined under Mexican law, the Court concluded that IBM had satisfied the “heavy” burden of establishing that a stay is warranted. IBM showed that there are issues common to the arbitration and the court proceeding, and that those issues will be finally determined by arbitration. And IBM further demonstrated to the Court’s satisfaction that it had not and would not take any steps to hamper the progress of the arbitration, that the arbitration may be expected to conclude within a reasonable time, and that any delay that might occur as a result of stay would not work undue hardship on Iusacell.

The Court’s decision contains at least four important lessons for practitioners.

First, U.S. courts are understandably suspicious of the motivations behind claims against nonparties to an arbitration agreement that duplicate the claims

at issue in a pending arbitration. And the more the party opposing the stay emphasizes its desire to use the court case to obtain discovery, the more pronounced those suspicions may become. As the Court noted, “it is hard not to conclude that Iusacell’s motivation for pursuing this action now is to gain tactical advantage in the arbitration.”

Second, courts will look closely at whether the positions taken by the parties in the arbitration are consistent with those taken in stay proceedings. The Court concluded, for example, that an agreed arbitration schedule with approximately a two-year timeline to decision was reasonable in light of the amount at stake and the complexity of the issues. In reaching that conclusion, the Court emphasized that the arbitration schedule was consistent with Iusacell’s preferences and proposed schedule, and that Iusacell had rejected an IBM México proposal that would have deleted from the arbitration agreement a procedural provision that Iusacell contended could generate potential delay.

Third, a stay decision need not be based on a conclusion that the arbitrators will resolve each and every issue in the related lawsuit. Thus, the fact that the arbitrators might not reach the Mexican law claim that Iusacell had asserted against IBM México in the arbitration and against IBM in the lawsuit did not counsel against a stay, where it was clear that the arbitrators would address the underlying premise of that claim, which involved IBM México’s performance under the MSA.

And, **fourth**, a party’s assertion of colorable defenses in the arbitration—including defenses that might limit the scope of the arbitration or the availability of discovery from the party seeking the stay—is not the equivalent of an attempt to hamper the arbitration. For example, the fact that IBM declined agreement to comply with discovery demands as though it was a party to the arbitration when the arbitral tribunal would not compel discovery of nonparties was not an obstruction of the arbitration.

Fourth Circuit *En Banc* Removal Victory for Colgate

In November 2014, the firm obtained a significant and ground-breaking victory for Colgate-Palmolive Co. in the U.S. Court of Appeals for the Fourth Circuit. That court, sitting *en banc*, became the first appellate court to hold that federal district courts have authority to vacate orders remanding cases to state court where those orders were procured by fraud, misrepresentations, or other misconduct.

The appeal arose after plaintiffs filed actions

against Colgate in the specialized asbestos docket in the Maryland Circuit Court for Baltimore City, seeking millions of dollars in damages for personal injuries under the novel theory—never accepted by any court or regulator—that Colgate’s Cashmere Bouquet cosmetic talcum powder contained asbestos that causes mesothelioma. Plaintiffs named a litany of defendants, including several defendants based in Maryland. After plaintiffs’ deposition testimony and discovery responses indicated that they had no evidence that their injuries might have been caused by any in-state defendant, Colgate removed the actions to federal court on the basis that plaintiffs had fraudulently joined the Maryland defendants to defeat federal jurisdiction. In federal court, plaintiffs’ counsel represented that plaintiffs had *bona fide* claims against the Maryland defendants that they intended to pursue, and thus sought remand to Maryland state court. The federal court remanded both cases based on these representations.

After securing remand on this basis, plaintiffs’ counsel immediately told the Circuit Court for Baltimore City that each case was a “one defendant case,” *disclaiming* both the existence of any evidence against an in-state defendant and any intention to pursue claims against those defendants. Colgate thereafter moved in federal court for sanctions and for relief from the remand orders pursuant to Fed. R. Civ. P. 60(b)(3), arguing that plaintiffs’ counsel had made misrepresentations regarding plaintiffs’ intention to pursue claims against the in-state defendants, solely for the purpose of defeating federal jurisdiction. The district court acknowledged that Colgate had raised “substantial” allegations and that the statements by plaintiffs’ counsel “appear to be in sharp conflict,” but nevertheless denied vacatur on the ground that it lacked jurisdiction in light of the prohibition in 28 U.S.C. § 1447(d) on “review[]” of certain orders granting remand to state court.

Colgate appealed, and a divided three-judge panel of the Fourth Circuit affirmed. Bolstered by a nearly 50-page dissenting opinion, Colgate sought rehearing *en banc*, which was quickly granted. The *en banc* court thereafter reversed, holding that vacatur of a remand order under Rule 60(b)(3) due to fraud, misrepresentations, or other misconduct does not constitute prohibited “review” of that order. The court of appeals explained that the distinction between “review” and “vacatur” is “not merely semantic” and that “Colgate seeks vacatur based on a collateral consideration—Colgate’s allegation that the remand orders were procured through attorney misconduct—rather than on the remands’ merits.” The court thus


reversed the district court’s determination that it lacked jurisdiction to vacate the remand orders, and it directed the district court to rule on Colgate’s motions on the merits. This important decision provides a powerful new tool for the defense bar and ensures that federal courts are not impotent when plaintiffs and their counsel seek to avoid federal jurisdiction through misconduct.

Victory for Megaupload

The firm obtained a major victory on behalf of its client, Megaupload Limited, in setting aside a restraint order that had been entered in the Hong Kong Special Administrative Region.

Following a criminal indictment filed in the United States against Megaupload Limited, the Secretary for Justice of Hong Kong, acting as an agent for the United States Department of Justice, submitted an *ex parte* application with the Court of First Instance of the Hong Kong High Court (the “Court”) to freeze the client’s assets located in Hong Kong. In January 2012, the Court granted the application and issued a restraint order freezing HK\$330 million (approximately US\$43 million) of the client’s assets.

In April 2014, Quinn Emanuel, through local counsel, filed an application with the Court to set aside the restraint order. The grounds for the set aside application included among other things that the Secretary for Justice breached its duty to make full and frank disclosure and duty of candor in relation to the Department of Justice’s inability to serve the criminal summons on the client in conformity with United States federal laws.

On December 4, 2014, the Court held that the failure to disclose such circumstance amounted to a material non-disclosure and thus set aside the restraint order. Further, the Court ordered that the costs of the application to set aside shall be paid by the Secretary for Justice. A new restraint order was granted, pending a new full trial on this issue, so the fight continues but the new restraint order should be subject to conditions much more favorable to Megaupload than the previous conditions. 

business litigation report

quinn emanuel urquhart & sullivan, llp

Published by Quinn Emanuel Urquhart & Sullivan, LLP as a service to clients and friends of the firm. It is written by the firm's attorneys. The Noted with Interest section is a digest of articles and other published material. If you would like a copy of anything summarized here, please contact Becca Voake at beccavoake@quinnemanuel.com.

- We are a business litigation firm of more than 700 lawyers — the largest in the world devoted solely to business litigation and arbitration.
- As of February 2015, we have tried over 2303 cases, winning 88.6% of them.
- When we represent defendants, our trial experience gets us better settlements or defense verdicts.
- When representing plaintiffs, our lawyers have garnered over \$42 billion in judgments and settlements.
- We have won four 9-figure jury verdicts.
- We have also obtained twenty 9-figure settlements and ten 10-figure settlements.

Prior results do not guarantee a similar outcome.

LOS ANGELES

865 S. Figueroa St., 10th Floor
Los Angeles, CA 90017
+1 213-443-3000

NEW YORK

51 Madison Ave., 22nd Floor
New York, NY 10010
+1 212-849-7000

SAN FRANCISCO

50 California St., 22nd Floor
San Francisco, CA 94111
+1 415-875-6600

SILICON VALLEY

555 Twin Dolphin Dr., 5th Floor
Redwood Shores, CA 94065
+1 650-801-5000

CHICAGO

500 W. Madison St., Suite 2450
Chicago, IL 60661
+1 312-705-7400

WASHINGTON, D.C.

777 6th Street NW, 11th Floor
Washington, DC 20001
+1 202-538-8000

HOUSTON

1001 Fannin St. Suite 1950
Houston, TX 77002
+1 713-224-4400

SEATTLE

600 University Street, Suite 2800
Seattle, WA 98101
+1 206-905-7000

TOKYO

NBF Hibiya Bldg., 25F
1-1-7, Uchisaiwai-cho, Chiyoda-ku
Tokyo 100-0011
Japan
+81 3 5510 1711

LONDON

One Fleet Place
London EC4M 7RA
United Kingdom
+44 20 7653 2000

MANNHEIM

Mollstraße 42
68165 Mannheim
Germany
+49 621 43298 6000

HAMBURG

An der Alster 3
20099 Hamburg
Germany
+49 40 89728 7000

MUNICH

Oberanger 28
80331 Munich
Germany
+49 89 20608 3000

PARIS

6 rue Lamennais
75008 Paris
France
+33 1 73 44 60 00

MOSCOW

Paveletskaya Plaza
Paveletskaya Square, 2/3
115054 Moscow
Russia
+7 499 277 1000

HONG KONG

1307-1308 Two Exchange Square
8 Connaught Place
Central Hong Kong
+852 3464 5600

SYDNEY

Level 15
111 Elizabeth Street
Sydney, NSW 2000
Australia
+61 2 9146 3500

BRUSSELS

rue Breydel 34
1040 Brussels
Belgium
+32 2 416 50 00