December 2013

quinn emanuel

quinn emanuel urquhart & sullivan, llp | business litigation report

los angeles | new york | san francisco | silicon valley | chicago | washington, d.c. | tokyo | london | mannheim | hamburg | munich | paris | moscow | hong kong | sydney

Wearable Computing—The Next Front in the Smartphone Wars?

The rapidly shrinking size of computer components and the development of high-speed wireless signaling technologies have made mobile computing devices ubiquitous. Users can now access data and applications from virtually anywhere. A new generation of wearable computing devices seeks to make access to technology even easier. The wearable computing market is expected to reach $10 billion by 2016, according to the research firm Gartner.

A number of different wearable computing technologies have recently emerged, with three categories of devices being especially prominent: smartwatches, smart glasses, and wearable fitness devices. Initially, the smartphone will serve as the network hub for many wearable devices, which will display information communicated by the smartphone. The current major smartphone makers have already adopted the Bluetooth Low Energy standard, which enables users to connect peripherals, like smartwatches and smart glasses, to their smartphones to access their data connection to the internet. As a result, the battle over the wearable computing market could very well divide along similar lines as the smartphone wars, with devices powered by Google's Android platform competing with devices utilizing Apple's iOS or Microsoft's Windows.

If the market for wearable computing devices expands as rapidly as predicted, incentives to litigate strategically will be present for players at all levels of the supply chain, from device manufacturers to chip makers. Much like the rise of the smartphone, the rise of wearable computing devices may generate a host of legal battles over intellectual property.

(continued on page 2)

INSIDE

Insurance Coverage for Cyber Attacks
Page 4

Practice Area Updates:

Trial Practice Update
Page 6

Structured Finance/Antitrust Update
Page 6

Russian Litigation Update
Page 7

Japanese Litigation Update
Page 8

German Federal Patent Court Invalidates One of Apple's Rubber Band Patents and Other Victories
Page 10

Quinn Emanuel London Sweeps in *Legal 500*'s United Kingdom Awards 2013

see page 5

Quinn Emanuel Named to *Law360*'s List of the "Most Feared Plaintiffs' Firms" and *The National Law Journal*'s "Plaintiffs' Hot List"

Quinn Emanuel has once again been named to *The National Law Journal*'s annual "Plaintiffs' Hot List," which recognizes the firms with the best track record representing plaintiffs in major business cases. The firm was selected for its bold strategy to sever ties with certain global financial institutions and major accounting firms in order to represent clients who had claims to bring against those institutions. Since then, Quinn Emanuel has become the leading firm worldwide in such representations and has won billions of dollars from the world's banking giants on behalf of clients such as the Federal Housing Finance Agency, Assured Guaranty Municipal Corp., and MBIA Insurance Corp. *Law360*, which described the firm as a "powerhouse in post-financial collapse litigation," also named the firm to its list of the "Most Feared Plaintiffs' Firms," an honor that comes directly on the heels of the firm's recognition as one of the "fearsome foursome"—the four firms in-house counsel fear the most in litigation (based on a poll of general counsel by BTI Consulting Group). Q

Faith Gay Receives 2013 Civic Leadership Award from Citizens Union of the City of New York

Citizens Union of the City of New York honored Quinn Emanuel partner Faith Gay with its prestigious 2013 Civic Leadership Award. Ms. Gay, who also serves as Co-Chair of the Firm's Trial Practice Group, is a nationally renowned trial lawyer with a long and successful record of public advocacy. Ms. Gay was honored for her work in advancing civil rights under law, equal access to justice, and full transparency in government. Q

Attorney Advertising

The Players

Among the tech giants, the wearable computing patent arms race is in full swing. Samsung, Apple, Google, Motorola Mobility, Microsoft, and HTC are actively seeking patent protection, acquiring patents to protect their valuable wearable computing technologies, and positioning themselves strategically to capture this emerging market. Anticipated wearable computing market entrants have also actively acquired smaller companies with wearable computing patent portfolios. For example, Jawbone recently acquired BodyMedia and its coveted biometric monitoring patent portfolio. Google acquired smartwatch developer WIMM Labs and its patents, and also a portfolio of smart glasses patents from Hon Hai.

Potential players with IP in the wearable computing space include at least the following companies:

Smart Glasses

- Google
- Samsung
- Apple
- Microsoft
- Vuzix
- Meta
- Lumus
- Recon Inst.
- Kopin Corp.
- Accenture
- Nikon
- Olympus
- Epson
- eMagin
- Carl Zeiss
- QD Laser
- Baidu
- Cal Tech

Smartwatches

- Samsung
- Sony
- Qualcomm
- Adidas
- HTC
- Google
- Apple
- IBM
- LG
- Asus
- Pebble
- Casio
- Comme Le Temps
- Hot
- Sonostar
- i'm SpA
- Martian
- Metawatch
- Rearden Tech

Wristbands/Fitness

- Jawbone
- Adidas
- Nike
- Fitbit Inc.
- Abbott Labs
- Medtronic
- Garmin
- Polar
- Suunto
- Leap Motion
- Thalmic Lab
- Bionym
- Weartech

Chips

- Broadcom
- Qualcomm
- IBM
- ST Micro
- MediaTek
- Marvell
- IBM
- ARM
- Intel
- AMD
- TI
- GreenPeak
- Himax
- Silver Spring
- Sensus USA
- Streetline
- InvenSense
- Alien Tech.
- Washington

Smart Glasses

Google Glass has attracted the most attention in the smart glasses category. In this exciting category, smart glasses are expected to augment reality, provide real-time information to consumers about their surroundings, and enable quicker and more seamless communications. Think of a world where your phone lets you know the name of the person whose name you should remember, and where people can avoid constantly turning to look down at their phones during meetings.

With Google Glass, consumers can keep their heads up and stay connected to reality while taking pictures, reading emails, surfing the Internet, following GPS navigation, and controlling the device through voice-activated and possibly gesture-based commands. While there are rumors of similar products from Microsoft and Samsung—but no public announcements—there are also a variety of other potential players, including Vunix with its M100 smart glasses, Recon Instruments' Jet sunglasses, which display fitness and map information and are designed for triathlon athletes, and Meta's SpaceGlasses, which feature two projection screens instead of one. Currently, the first round of glass products are all expected to ship to consumers in 2014.

Smartwatches

Among the tech giants, Samsung and Sony have taken the lead and recent headlines with their respective releases of the Galaxy Gear smartwatch and the Sony SmartWatch MN2.

Users receive emails, texts, and phone calls right on their wrist. By keeping the smartphone in the user's pocket for basic tasks like reading emails, the smartphones battery life is saved. Smartphone-integrated watches have been released, announced, or rumored to be in development, by Samsung (Galaxy Gear), Sony (SmartWatch MN2), Apple, Google, and a multitude of start-ups, including Kickstarter-funded Pebble Technology and a spinoff of the Fossil watch brand called MetaWatch.

Health Monitoring Wristbands

Other companies are producing popular health-monitoring wristbands and apps, such as Jawbone (UP), Adidas (miCoach), Fitbit (Flex), and Nike (FuelBand). It's possible that the smartwatch and wristband markets will merge over time, as the health wristbands develop deeper smartphone integration, and as the smartwatches include more health monitoring features. For example, Adidas recently announced a miCoach Fitness Smartwatch. Similarly,

the Pebble smartwatch, announced in November that it will incorporate fitness monitoring into its next generation of smartwatch technology, and Samsung's Galaxy Gear already contains health monitoring functionality through its S Health tracking app.

Chip Makers

Because Bluetooth technology enables easy, low-power connectivity between Android and iOS phones with wearable computing accessories, some segments of the market may have low barriers to entry and be ripe for startup innovation. Recently the CEO of chip maker Broadcom explained that, "There are two companies that make the bulk of smartphones today. But there are potentially thousands and thousands of little companies that can make wearables." "These may be watches, rings, dog collars—these kinds of wearables can be made not for millions of dollars or hundreds of thousands of dollars, but for tens of thousands or even less. You could do it on your credit card." Broadcom, and its fellow chip manufacturers Qualcomm, Intel, AMD, Marvell, Mediatek, ST Micro, and others, stand to benefit by offering chips and connectivity platforms which wearable startups can utilize. It is expected, particularly in the health and fitness space, that additional wearable accessories will continue to be developed, relying on the same basic operating system, Bluetooth, and communications platforms.

The Next Front

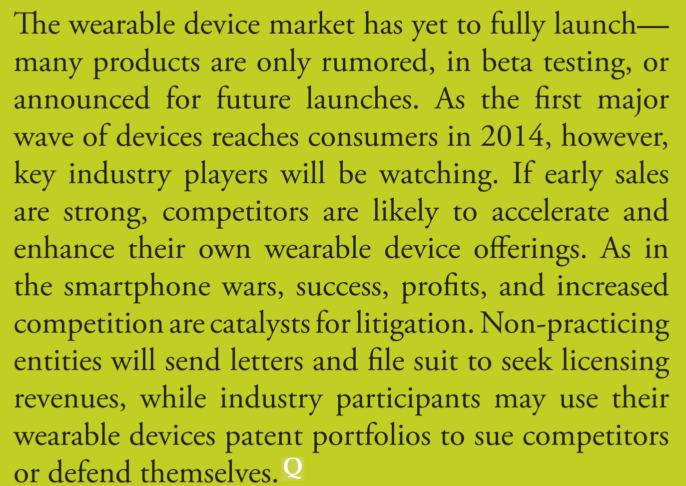
As wearable computing becomes a reality, will the tech giants learn from the smartphone wars or will they double down on their current strategies? It was Apple that famously declared "thermonuclear war" and set out to "destroy Android." But far from destroying Android, today the most profitable handset vendor is Samsung, and Google's Android is the top mobile operating system. As one commentator succinctly put it:

If Apple's legal maneuvers were intended to curtail or at least slow down the growth of Android, then they have been an abject failure so far.

Despite the lack of demonstrable effects on the marketplace, however, litigation regarding smartphones, tablets, and other mobile computing devices continues at a brisk pace. There is little reason to doubt that the tech giants will continue to use all the tools at their disposal—including intellectual property—to secure their share of this growing market.

Patent litigation tends to follow the money—and wearable computing should be no exception. That means that, in addition to litigation between industry heavyweights, there is also likely to be intellectual property litigation regarding wearable devices brought by non-practicing entities ("NPEs"). An NPE named SportBrain has already sued Adidas, Fitbit, and Nike over a patent titled, "Integrating personal data capturing functionality into a portable computing device and a wireless communication device." SportBrain apparently existed over a decade ago, but went out of business. But its patent remains. As Congress considers legislation directed to addressing NPE litigation, failed startups and other NPEs like SportBrain are sure to feature in the coming wearable computing patent wars.

Conclusion



The wearable device market has yet to fully launch—many products are only rumored, in beta testing, or announced for future launches. As the first major wave of devices reaches consumers in 2014, however, key industry players will be watching. If early sales are strong, competitors are likely to accelerate and enhance their own wearable device offerings. As in the smartphone wars, success, profits, and increased competition are catalysts for litigation. Non-practicing entities will send letters and file suit to seek licensing revenues, while industry participants may use their wearable devices patent portfolios to sue competitors or defend themselves. Q

Insurance Coverage for Cyber Attacks

Thefts of trade secrets through cyber espionage and cyber harassment through distributed denial of service attacks have been business hazards for years. Cyber security insurance policies to guard against these threats have been available since the 1970s. More recently, however, true cyber *attacks* have been capable of causing real-world harm. In FBI Director James Comey's first Congressional testimony, he warned that cyber attacks surpass terrorism as the primary threat against the United States. This threat is by no means limited to the United States.

In 2010, malware researchers discovered a computer worm called "Stuxnet." Further investigation revealed that the program would spread indiscriminately, but had a very specific target: the industrial control systems used in Iran's nuclear program. The worm, it was reported, damaged industrial equipment and interfered with production processes in Iran, while, at the same time, it reported false data to the control systems so that they reported no errors to the operators. This discovery has been described as "an Oppenheimer moment in the history of hacking."

Malicious programs like Stuxnet can interfere with the supervisory control and data acquisition (SCADA) software on industrial control systems, while giving their users the false impression that all is well. Stuxnet's progeny could target the SCADA interfaces on air traffic control systems, on dams, on the electrical grid, or on the energy distribution or storage facilities, among others. Most dangerous would be attacks on the control systems of chemical, food processing, nuclear or water treatment plants.

This article addresses the legal consequences for insurers and insureds in the event of such an unprecedented, but possible, event.

At a Department of Homeland Security National Protection and Programs Directorate Cyber Security Insurance Workshop in November 2012, a federal official stated that "companies should not assume that the federal government will take responsibility" as the insurer of last resort in a catastrophic cyber attack, unless the government first "requires them to adopt a particular security solution prior to a successful attack." Even then, "it's unclear that the government would own the liability."

In 2002, the Terrorist Risk Insurance Program Act (TRIA) became law. TRIA sought to provide "for a transparent system of shared public and private compensation for insured losses resulting from acts of terrorism," to protect consumers, ensure the availability and affordability of terrorism risk insurance, stabilize markets, and "build capacity to absorb any future losses." TRIA defines terrorism as a violent act dangerous to human life, property or infrastructure, occurring within the US (or to a US air carrier, vessel or diplomatic facility), committed on behalf of a foreign person or interest, to coerce the American people or United States Government. Crucially, the act must be certified as terrorism by the Secretary of the Treasury, a determination not subject to judicial review. Such a certification creates a private cause of action for property damage, injury or death. TRIA, however, expires on December 31, 2014. Neither TRIA nor the draft TRIA reauthorization bills before Congress, discuss cyber security, much less cyber attack. While some in the insurance industry believe the Department of Treasury has informally indicated that it would certify a cyber attack as terrorism covered by TRIA, this is not clear, and efforts are underway to make explicit such a guarantee.

Industry and insurance representatives disagree over whether existing cyber insurance policies would cover physical damage from Stuxnet-type attacks, whether stand-alone policies on SCADA systems are needed, or whether traditional casualty and property insurance would cover losses incurred in a cyber attack. Some general liability policies exclude cyber incidents from coverage.

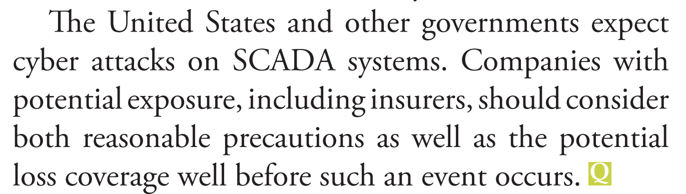
A response by the United States government to the threat of cyber attack is beginning to take shape, which will impact businesses in as-yet unpredictable ways. In February, President Obama's Executive Order 13636 warned that the "cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." That same month, pursuant to Presidential Policy Directive 21, DHS identified infrastructure "where a cyber security incident could reasonably result in catastrophic regional or national effects…" DHS named 16 such sectors in a list that encompasses significant segments of the economy: the agricultural, chemical, commercial, communications, dams, defense, emergency services, energy, financial, government, healthcare, information technology, manufacturing, nuclear, transportation and wastewater sectors.

In addition, a "voluntary" cyber security framework will be issued by the Department of Commerce next February. After a meeting between President Obama and corporate chief executives this October, the White

House stated that the framework being created by the National Institute of Standards and Technology (NIST) is "intended to raise the level of cyber security across the U.S. critical infrastructure," and "will lay out a set of core practices for organizations to manage their cyber security risk." The same day, the NIST released for comment a framework for businesses to use in identifying, protecting against, detecting, responding to and recovering from cyber threats. The goal is to establish standards and best practices. The framework highlights legal and regulatory requirements, as well as methodologies, for protecting privacy and civil liberties. A possible implication of these forthcoming standards and best practices is that industries which do not follow these guidelines will have not met minimum standards of care. Business will need to adapt to these guidelines, and insurers will need to become familiar with them.

When a cyber attack on a SCADA system occurs, then the parties to insurance litigation in the aftermath will have to grapple with a number of novel issues:

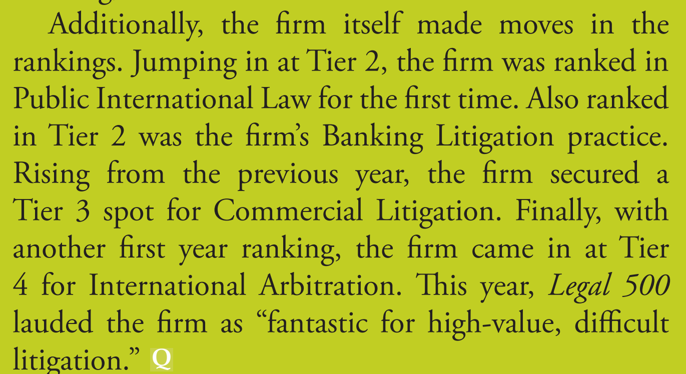
- A computer virus is difficult to attribute positively to an individual, and possible to misattribute, frustrating efforts to identify for the purposes of TRIA the foreign actor responsible. In addition, a Stuxnet-type attack can be launched from anywhere in the world, potentially complicating the requirement that the act take place in the US.
- Senior Iranian security officials have publicly singled out the US power grid as vulnerable to retaliation, in response for what has been described in the press as an American and Israeli effort to use Stuxnet to attack Tehran's suspected nuclear arms program. Iran often acts through non-state actors, such as Hezbollah. Query whether, given the international political implications, a Treasury Secretary would be willing to certify, for the benefit of a civil action brought by a private party, that Iran committed an act of war against the United States through a proxy.
- The recent Executive Order suggests intelligence indicating the likelihood of a cyber attack on identified US public and private infrastructure. While the US government is involving business more closely in cyber security, intelligence reporting on this subject is sensitive by its nature, and shared by the government with certain industry partners in a highly sanitized fashion, when it is shared at all. It is not clear whether cyber security intelligence is shared with the insurance industry.



The United States and other governments expect cyber attacks on SCADA systems. Companies with potential exposure, including insurers, should consider both reasonable precautions as well as the potential loss coverage well before such an event occurs. Q

Quinn Emanuel London Sweeps in *Legal 500*'s United Kingdom Awards 2013

Six attorneys from the firm's London office were recently recognized as Leading Individuals in key business litigation practice areas in *Legal 500*'s United Kingdom Awards 2013. Richard East ("highly rated") and Sue Prevezer QC ("a wonderful lawyer"), co-managing partners of the London office, were both identified as Leading Individuals in the areas of Commercial Litigation and Banking Litigation. Newly-joined partner Ted Greeno was recognized for Commercial Litigation. Stephen Jagusch, Global Chair of Quinn Emanuel's International Arbitration Practice, helped the firm receive its first individual recognitions in the areas of International Arbitration and Public International Law. Along with Jagusch, Anthony Sinclair was also recognized as a leader in Public International Law. Robert Hickmott was recognized as a top practitioner in Corporate Restructuring and Insolvency. Among other attorneys recognized by the publication were Alex Gerbi, Martin Davies, Matthew Bunting, and Marc Becker.



Additionally, the firm itself made moves in the rankings. Jumping in at Tier 2, the firm was ranked in Public International Law for the first time. Also ranked in Tier 2 was the firm's Banking Litigation practice. Rising from the previous year, the firm secured a Tier 3 spot for Commercial Litigation. Finally, with another first year ranking, the firm came in at Tier 4 for International Arbitration. This year, *Legal 500* lauded the firm as "fantastic for high-value, difficult litigation." Q

Trial Practice Update

Ninth Circuit Appeal Raises Questions Whether* Batson *Forbids Sexual Orientation-Based Peremptories. Can you strike a prospective juror simply because he is gay? A small number of states, including California, prohibit peremptory challenges based on sexual orientation, but the issue is unsettled in most jurisdictions, including in the federal courts. A case now pending in the Ninth Circuit, *Smithkline Beecham Corporation v. Abbott Laboratories*, 11-17357, 11-17373, presents this question of first impression regarding the exercise of peremptory challenges. Such challenges to prospective jurors are generally completely discretionary, but in *Batson v. Kentucky*, 476 U.S. 79 (1986), the Supreme Court held that peremptories may not be based on race. The Court extended *Batson* to forbid the exercise of sex-based challenges in *J.E.B. v. Alabama*, 511 U.S. 127 (1994).

Under *Batson*, once the opponent of a peremptory challenge makes a prima facie case of discrimination—which requires demonstrating (1) membership in a cognizable group, (2) use of a peremptory, and (3) an inference, based on the totality of the circumstances, that the strike was motivated by group membership—the burden shifts to the proponent of the strike to come forward with a non-discriminatory explanation. The explanation need not be "persuasive, or even plausible;" unless a discriminatory intent is "inherent" in the explanation, the explanation will suffice. Once any non-discriminatory explanation is offered, the trial court decides whether the opponent of the strike has proved purposeful, forbidden discrimination.

The question whether *Batson* forbids peremptory strikes based on sexual orientation now before the Ninth Circuit arose out of a case concerning the alleged attempted monopolization of the market for a certain type of HIV/AIDS therapy, which went to trial in 2011 in the Northern District of California. During jury selection, a male juror revealed that he was gay by openly discussing the employment history of his male partner. A lawyer for the defense used a peremptory strike to remove him from the jury pool. Plaintiff's counsel objected, saying the juror "is or appears to be, could be, homosexual," and that the defense had used its challenge to exclude him because the litigation involved a controversial price increase for AIDS medications, which are of special significance to the gay community. Following the *Batson* objection, (now Chief) Judge Claudia Wilken provided the defense lawyer the opportunity to offer a neutral rationale for his strike, but the lawyer stated only he had "no idea whether [the juror] is gay or not," and opted to stand on several (incorrect) legal justifications Judge Wilken gave—such as *Batson*'s inapplicability to civil cases—for rejecting the *Batson* challenge. The jury returned a mixed verdict and the parties cross-appealed; the *Batson* issue features prominently in the briefing on appeal.

On September 18, 2013, a panel of the Ninth Circuit composed of Judges Schroeder, Reinhardt, Berzon, heard argument and appeared receptive to several of the plaintiff's arguments that *Batson* applies to sexual orientation. The panel expressed skepticism that ordinary rational basis review should apply in an equal protection challenge to discrimination against gays and lesbians in light of the recent Supreme Court gay marriage case, *United States v. Windsor*. The panel also appeared unsure it would be proper to consider the "neutral" justifications for the strike proffered by defense counsel on appeal, given that none were stated at trial and they could have been carefully manufactured in the interim. A ruling is expected in the next few weeks or months.

Structured Finance/Antitrust Update

Major Banks Face New Antitrust Investigations and Civil Suits. On the heels of the investigations into manipulation of LIBOR and price-fixing in the aluminum markets, the world's largest banking institutions now face new inquiries from domestic and international antitrust regulators into allegations of manipulation of the foreign currency exchange ("FX") market. These investigations have raised the possibility of a new wave of lawsuits. Two class action suits alleging antitrust violations based on FX manipulation and collusive conduct have already been filed, and additional class actions and/or individual suits are likely to follow.

The currency exchange market is a $5.3-trillion-a-day market—the largest in the financial system. Companies, investors, portfolio managers, and stock index compilers, among others, use exchange-rate benchmarks—snapshots of traded currency rates calculated on a half-hourly or a hourly basis using sample data from a minute-long period starting thirty seconds before the half-hour/hour mark—as a transparent and auditable way of buying and selling currencies. The most popular benchmark, called the WM/Reuters rate or the "London fix," runs at 4 p.m. London time on each trading day. Roughly 1% to 2% of overall global foreign exchange transactions are conducted at this "fix." The foreign exchange market is largely opaque and almost entirely unregulated, with four banks dominating the market and trading around the "London fix": Deutsche Bank AG (15.2%), Citigroup Inc. (14.9%), Barclays Plc (10.2%) and UBS AG (10.1%). Collectively, these banks have a market share greater than fifty percent.

On June 12, 2013, *Bloomberg News* published an exclusive report, citing five confidential dealers, that traders "at some of the world's biggest banks manipulated

foreign-exchange rates used to set the value of trillions of dollars of investments." Since then, the Financial Conduct Authority of the United Kingdom, the Swiss Financial Market Supervisory Authority, and Joaquin Almunia of the European Commission's competition group have announced investigations into the practices by major banks. On October 9, 2013, the Swiss Finance Minister claimed at a briefing on the investigation that it is "a fact that currency manipulations have been committed." The U.S. Commodity Futures Trading Commission has also been reviewing potential violations of the law with respect to currency markets, and the U.S. Department of Justice has opened a criminal investigation into manipulation of the foreign exchange market.

The investigations focus on allegations that traders at major banks such as Deutsche Bank AG, Citigroup Inc., Barclays Plc, Goldman Sachs, HSBC, JPMorgan, Standard Chartered, UBS AG, and Royal Bank of Scotland have been conspiring to manipulate the WM/Reuters foreign-exchange benchmark rate that is fixed at 4 p.m. in London. Countless transactions executed by these banks are tied to this benchmark rate, and traders are alleged to have frequently "front-run" their clients' transactions to make a profit. It has been reported that, by conspiring to manipulate the benchmark, these banks *ensure* they always win these "front-running bets," costing their clients millions if not more.

To ensure that their front-running is successful, and to maximize their profits at their clients' expense, traders have allegedly conspired to artificially influence the benchmark rate in one direction. According to confidential sources, traders at rival banks send instant messages to each other on a routine basis when respective client orders match up enough to allow for rate-setting. This group of traders was known by various monikers, including "The Cartel." Two sources reportedly told *Bloomberg News* that traders "would share details of orders with brokers and counterparts at banks through instant messages to align their strategies" and "to glean information about impending trades to improve their chances of getting the desired move in the benchmark." By concentrating orders in the moments before and during the 60-second benchmark window, traders can push the rate up or down, a process known as "banging the close." To maximize these profits, dealers reportedly buy or sell client orders in installments during the 60-second window to exert the most pressure possible on the published rate. Since the rate is based on the median of transactions during the period, placing a number of smaller trades could have a greater impact than one big deal. Given the size of the FX market, even minor movements in the benchmark rate can mean millions of dollars in profits for traders with inside knowledge.

Quantitative studies of the foreign exchange market appear to confirm the anecdotal accounts of traders. In the 30 minutes preceding the "London fix" at 4 p.m., certain currencies regularly experience significant price spikes followed by quick reversals after calculation of the benchmark. Data regarding the number of times spikes of at least 0.2 percent occurred in the 30 minutes before the 4 p.m. benchmark on the last working day of each month from July 2011 through June 2013 suggest that collusion has occurred.

Two class actions alleging illegal antitrust conspiracies have recently been filed in U.S. District Court for the Southern District of New York. The first is brought by Haverhill Retirement System, a retirement fund for public sector employees, and alleges that a class of investors that entered into foreign currency trades directly with the Defendant banks was harmed by the Defendants' manipulation of FX rates. The complaint defines the class to include "all persons who traded foreign currency directly with a Defendant in the United States between August 1, 2005 and the present which transaction was settled on the basis of WM/Reuters Rates." Similarly, a second class action brought by a Korean company, Simmtech Co. Ltd., includes substantively identical factual allegations, but defines the class to include all persons in the Republic of Korea who entered into foreign currency transactions directly with a defendant, which transaction was settled on the basis of WM/Reuters Rates. Both complaints assert causes of action for violation of Section 1 of the Sherman Act; the Simmtech complaint also includes two state law claims, for violation of New York General Business Law, §§ 340 and 349.

Given the size of the FX market and the ongoing investigations, additional class action and individual lawsuits are expected.

Russian Litigation Update

Russian Courts on Anti-Suit Injunctions. More than a year ago Anton Ivanov, the Chairman of the Supreme Arbitrazh Court, openly criticized foreign anti-suit injunctions affecting Russian proceedings as an example of "unfair competition" between judicial systems. In this context, it is interesting to consider the approach adopted in Russian case law to foreign anti-suit injunctions and to obtaining similar injunctions in Russian courts.

Foreign Anti-Suit Injunctions in the Russian Case Law. In the beginning, the attitude of Russian courts to anti-suit injunctions from foreign courts was rather hostile. In *Roust Holdings Ltd. v. Cetelem SA* (2005), the Russian court declared that the English anti-suit injunction obtained by Cetelem SA in support of an ICC injunction in London violated the constitutional right for

judicial protection and could not be enforced in Russia. The court requested that the parties pursue the case in Russia and noted that any actions to the contrary would be regarded as contempt of court. Shortly afterwards, the parties settled the dispute.

Subsequently, Russian courts adopted a more measured approach to foreign anti-suit injunctions. In *JFC Group Ltd. v. Star Reefers Pool Inc.* (2010), JFC Group Ltd. filed a motion to stay Russian proceedings on the basis of the anti-suit injunction issued by the High Court of Justice (England). The court granted the motion and ordered JFC Group Ltd. to notify the court of any changes relating to anti-suit injunction. Interestingly, a year later JFC Group Ltd. notified the Russian court that the anti-suit injunction was still in place, but this time the Russian court resumed proceedings and continued with merits of the case, though JFC Group Ltd. could not take part in the proceedings because of the injunction.

A relatively measured approach to foreign anti-suit injunctions was taken in *Ingosstrakh Investments v. BNP Paribas SA and OJSC Russian Machines*. BNP Paribas brought an LCIA case against Oleg Deripaska's Russian Machines seeking enforcement of a guarantee issued by Russian Machines to BNP Paribas. After that, a minority shareholder of Russian Machines, represented by its trustee Ingosstrakh Investments, initiated Russian proceedings against BNP Paribas and Russian Machines, seeking invalidation of the guarantee. BNP Paribas obtained an anti-suit injunction prohibiting Russian Machines and Ingosstrakh Investments from pursuing the claim in Russia. By the time the injunction was granted, the Russian court had already delivered a judgment and declared the validity of the guarantee, and Ingosstrakh Investments had already appealed that judgment. In these circumstances, Ingosstrakh Investments and Russian Machines moved for a hearing *in absentia* in the Russian appellate court, which affirmed the validity of the guarantee in their absence. The defeated party lodged a cassation appeal. In the cassation hearing BNP Paribas tried to challenge the jurisdiction of the court based on an active interim order against the parties. The Russian cassation court rejected this argument, proceeded to consider the case with BNP Paribas being the only party in attendance, and also affirmed the validity of the guarantee.

On July 9, 2013, the Presidium of the Supreme Arbitrazh Court of the Russian Federation (the "Presidium") issued Clarifications on the court practice on cases involving foreign parties. The BNP Paribas case served as a basis for clarification. The Presidium stated that "*anti-suit injunctions issued by a foreign court cannot prevent a case from being considered by a Russian court that has jurisdiction to hear the case.*"

The key conclusions drawn by the Presidium are the following:

- all states are equal and sovereign, and a court of one state cannot impose restrictions on a court of a different state;
- an anti-suit injunction issued by a foreign court does not prevent a Russian court from considering the case and does not have other legal effects in Russia; and
- anti-suit injunction, however, binds the parties, and they should weigh the risks and implications of non-compliance with the anti-suit injunction.

At the same time the Supreme Arbitrazh Court has not expressed a view on anti-suit injunctions from Russian courts. We will consider this issue below.

Anti-Suit Injunctions by Russian Courts. Russian law does not specifically provide for anti-suit injunctions. A Russian court, however, may grant injunctive relief provided that:

- the interim relief sought is related to and corresponds to the subject-matter of the dispute; and
- failure to apply the interim relief may impede or render impossible the enforcement of future judgment, or is likely to inflict substantial harm to the applicant.

The issue of the anti-suit injunction had already arisen in Russian proceedings. In August 2012, the Arbitrazh Court of the City of Moscow considered an application for anti-suit injunction in a case between Novolipetsk Metallurgical Plant and Mr. Nikolay Maximov and his JSC Maxi-Group. Dismissing the application, the court ruled that the injunction sought was not related to the subject matter of the dispute and that denying the injunction would not prevent enforcement of a future judgment. Although the court dismissed the application on formal grounds, it did not rule, as a matter of principle, on the power of Russian courts to issue anti-suit injunctions.

In summary, since July 9, 2013, Russian courts have been given guidance on how to deal with foreign anti-suit injunctions. Time will tell how this guidance will be applied in practice. Meanwhile, other parties will attempt to obtain anti-suit injunctions from Russian courts. Whether they will be successful is a question yet to be answered.

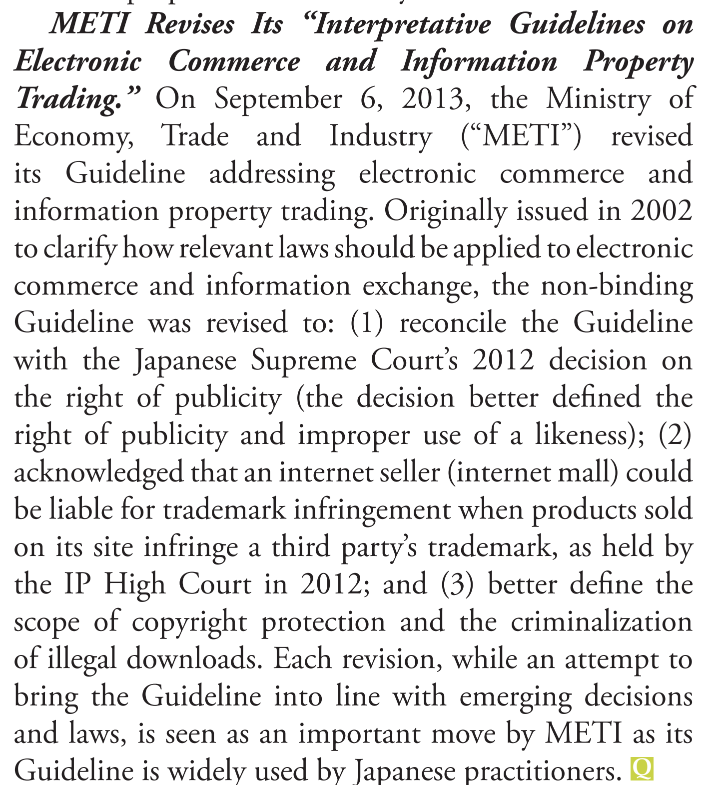
Japanese Litigation Update

Japanese Government Tightens Insider Trading Regulations. On June 12, 2013, the Japanese Diet passed an amendment to the Japanese Financial Instruments and Exchange Act, including enhancements of many insider trading regulations. One change drawing attention is the

strengthening of the law governing use of unpublished information with respect to third parties. Specifically, under the new regulation, a corporate insider—such as an officer or employee of a listed company or a managing underwriter—who learns an unpublished material fact regarding the listed company in the course of his/her duty is now prohibited from disclosing that information to a third party or soliciting a third party for the purpose of promoting the interest of that third party. Rather than seek to protect third parties, the regulation focuses on preventing the improper disclosure of information to third parties and ensuring the fairness and soundness of the securities market. The solicitation of the third party is therefore prohibited even if no insider information is actually disclosed. If the third party actually makes a sale based on the insider information, the person that provided the information or solicited that third party shall face imprisonment (with a five-year maximum sentence) and/or a fine not to exceed 5 million yen (approximately $50,000), and/or other fines. In addition, the guilty party's name will be published. Moreover, if an officer or employee of a company breaches the regulation in the course of his/her work, the company is also liable. The amendments will take effect by June 19, 2014.

Intellectual Property High Court Expands Recovery for Non-Practicing Patent Holder. On February 1, 2013, the Grand Panel of Intellectual Property High Court ("IP High Court") issued a judgment expanding the scope of Article 102, paragraph (2) of the Patent Act ("102(2)") as it applies to entities not practicing their patent in Japan. Under Article 102(2), damages for patent infringement are presumed to be the amount of profit earned by the infringer. Numerous lower courts, including the decision of the Tokyo District Court from which the appeal originated, held that only a patentee that practiced his invention could claim presumed damages under Article 102(2). The IP High Court, however, reversed this decision and held that practicing one's patent is not required to seek presumed damages under Article 102(2). Rather, a patentee could claim damages under Article 102(2) if the infringement harmed the patentee's ability to obtain profits from the patent. In the case itself, the court awarded damages under the provision to a United Kingdom company that did not practice its patent in Japan, but did sell products through a distributor. By allowing the plaintiff to use Article 102(2), the decision increased the damage award by approximately seven times. It remains to be seen how Article 102(2) will be applied to a true non-practicing entity that only holds patents and does not sell products in the market at all.

Japanese Cabinet Approves New Bill Introducing a "Japanese Class Action." A new bill recognizing a special civil procedure for collective recovery of consumers' damages was approved by the Cabinet and submitted to the House of Representative in Japan (*Shugi-in*) on April 19, 2013. Scholars and practitioners are watching with interest as this furthers the introduction of a Japanese version of a limited class action suit. The bill will be discussed and considered in the Diet session starting in mid-October. This bill allows Specified Qualified Consumer Organizations ("SQCO," a special type of Qualified Consumer Organization)—groups that must fulfill a number of requirements in order to be deemed a SQCO—to seek certain types of damages and restitution from consumer contracts on behalf of a number of individuals. The consumer contract is defined as a contract between an individual consumer and a business operator, excluding employment contracts. The proposed system consists of two phases. In phase one, a SQCO would file a declaratory judgment action asserting that a business operator has not fulfilled a monetary obligation to a substantial number of consumers who share common factual and legal grounds for recovery, based in contract. In the second phase, the court would assess the validity and amount of the individual consumer's claims, provided the plaintiffs opted in to the class. The decision would also apply the first stage decision to SQCOs that did not participate in the first-stage procedure so as to prevent multiple lawsuits on the same issue. Consequential damages, lost profits, personal injury, and pain and suffering are categorically excluded from the proposed class action system.



METI Revises Its "Interpretative Guidelines on Electronic Commerce and Information Property Trading." On September 6, 2013, the Ministry of Economy, Trade and Industry ("METI") revised its Guideline addressing electronic commerce and information property trading. Originally issued in 2002 to clarify how relevant laws should be applied to electronic commerce and information exchange, the non-binding Guideline was revised to: (1) reconcile the Guideline with the Japanese Supreme Court's 2012 decision on the right of publicity (the decision better defined the right of publicity and improper use of a likeness); (2) acknowledged that an internet seller (internet mall) could be liable for trademark infringement when products sold on its site infringe a third party's trademark, as held by the IP High Court in 2012; and (3) better define the scope of copyright protection and the criminalization of illegal downloads. Each revision, while an attempt to bring the Guideline into line with emerging decisions and laws, is seen as an important move by METI as its Guideline is widely used by Japanese practitioners.

German Federal Patent Court Invalidates One of Apple's Rubber Band Patents

The firm obtained a victory for Motorola in the German nullity proceedings against a member of Apple's rubber band patent family (EP 2 059 868, *"Portable Electronic Device for Photo Management"*) before the German Federal Patent Court. The patent relates to the bounce back functionality that is used in various smart phone applications such as photo gallery. Apple had sued most of the Android manufacturers based on this patent in Germany.

The firm successfully argued that the patent could not claim all seven priorities specified in the patent, making a video-documented presentation of Apple's co-founder Steve Jobs with the original iPhone in 2007 (Keynote Macworld, SF), which had been identified and submitted by the QE team, prior art. Unlike US patent law, neither the European Patent Convention (EPC) nor German patent law provide for a grace period to cure the consequences of an inconsiderate publication or public use of the invention by the patent applicant or inventor before the actual patent application. Paving the way for a solid argument on inventive step (obviousness) based on the iPhone presentation, the Court nullified the patent in its entirety (decision appealable).

The firm represents Motorola not only in the nullity action, but also in the respective infringement proceedings. (Germany has a bifurcated system and the infringement court must not decide on the validity of an asserted patent.) Based on the revocation of the patent in suit, the infringement court has to consider a stay of the proceedings pending a final nullity decision.

Quinn Emanuel Obtains Re-Trial for Woman Sentenced to 20 Years for Firing Warning Shot

In an important *pro bono* victory, Quinn Emanuel succeeded before Florida's First District Court of Appeal in obtaining reversal of the conviction of Marissa Alexander, a 31-year-old Florida mother of three who was convicted of aggravated assault with a deadly weapon and sentenced to a mandatory minimum of twenty years under Florida's "10-20-Life" statute. Alexander, a victim of serial spousal abuse, was forced to fire a warning shot to ward off an attack from her husband in her own home. Alexander was denied immunity under Florida's Stand Your Ground law by the trial court on the ground that she could have fled from her home instead of firing her weapon. At trial, she argued that she had acted in self-defense. The jury returned a guilty verdict and she was sentenced to a mandatory 20 years despite having no prior record.

Quinn Emanuel entered the case at the appellate stage. After scouring the record, Quinn Emanuel's attorneys identified two significant errors in the jury instructions given regarding Alexander's claim of self-defense. First, the jury was instructed that, in order to find that she had acted in self-defense, Alexander was required to prove beyond a reasonable doubt that she was in fear of an aggravated battery by her spouse, when it is the State's burden as a matter of law to prove that Alexander did not act in self defense. Second, the jury was instructed that Alexander could not have acted in self-defense unless the victim suffered "injury." Plainly, no one had been injured by her warning shot. As the jury instructions given were, in fact, the standard instructions approved for use generally by the Florida Supreme Court, it was incumbent on Quinn Emanuel to argue why, in Alexander's case, those standard instructions were inapplicable, and, in fact, undermined her assertion of self-defense.

On September 26, 2013, the First District issued an order reversing Alexander's conviction and remanding for a new trial. It agreed with Quinn Emanuel that the jury instructions were fundamentally flawed in both respects, and that, because both the defense and the prosecution had argued at trial that the jury's only question was whether Alexander had acted in self-defense, the flawed jury instructions had deprived Alexander of a fair trial.

Quinn Emanuel intends to seek bail for Alexander, and will represent her at her re-trial.

Fortinet and Quinn Emanuel Torch Patent Troll

The firm was proud to represent Fortinet, Inc., a publicly traded network-security company, in patent litigation against a non-practicing entity, NPS. In litigation pending in federal court in Northern California, NPS targeted Fortinet's franchise product line, FortiGate firewall products, and sought damages of over $18 million, trebled to over $50 million. The firm succeeded in procuring numerous court orders finding that NPS had engaged in litigation misconduct, including attempts to conceal evidence and making false or misleading statements to the Court. The firm also succeeded in procuring a court order excluding NPS's damages expert from trial. In the face of those rulings, NPS agreed to abandon its campaign outright. The case was dismissed with prejudice and—as disclosed in Fortinet's recent SEC filing—Fortinet paid nothing at all to NPS for that result. This was a complete win for Fortinet. It was reported widely by *Law360*, *Courthouse News*, *TechDirt* and *Network World*.

Victory for Sandoz in $500 Million Securities Action

On August 7, 2013, Quinn Emanuel obtained a victory for four clients, Sandoz AG, Sandoz International GmbH and two individuals, by securing dismissal on constitutional standing grounds of eleven federal and state securities, breach of contract, and negligent misrepresentation claims filed against them in the United States District Court for the Southern District of New York by Shareholder Representative Services LLC ("SRS"). SRS, a stockholder representative that frequently acts on behalf of the former shareholders of entities that are sold through mergers and acquisitions, brought the claims in connection with a merger agreement between the former shareholders of an entity that was acquired by one of the defendants, Sandoz Inc., in 2010. Because stockholder representatives like SRS are regularly involved in M&A activity, the decision to dismiss SRS's complaint in its entirety for lack of standing is likely to have broad implications for other stockholder representatives wishing to pursue litigation on behalf of former shareholders in federal court.

The merger agreement was signed by SRS on behalf of the shareholders, expressly granted SRS the right to "assert any claims" on behalf of the shareholders, and named SRS as the shareholders' agent and attorney in fact. The court's ruling dismissing the claims hinged on the fact that SRS failed to allege that it suffered an injury-in-fact at the time it filed the complaint and sought instead to raise the injuries and legal rights of the former shareholders. Significantly, the court found that neither the original complaint nor the two amended complaints, which SRS filed after it obtained claim assignments from some of the former shareholders, identified a concrete and particularized injury that was suffered by SRS as opposed to its clients. Rather, as the court acknowledged, SRS's role in the underlying events concerning the merger, and at the time it first filed the lawsuit, "was that of 'agent and true and lawful attorney-in-fact'" for the former shareholders—a role that, "without more, d[id] not convert the injuries allegedly suffered by the Shareholders into SRS's own injuries." *Shareholder Representative Services LLC v. Sandoz Inc., et al.*, No. 12-cv-6154 (DLC), Opinion & Order at 18-19 (S.D.N.Y. Aug. 7, 2013) (citing *W.R. Huff Asset Mgmt. Co. v. Deloitte & Touche LLP*, 549 F.3d 100, 107-08 (2d Cir. 2008)). The court rejected SRS's contention that the former shareholders' post-filing assignment of their claims to SRS cured any standing defects that may have existed when it first filed the case because, among other reasons, Federal Rules of Civil Procedure 17(a)(3) and 15(c) permit an amended complaint to relate back to the original filing of the complaint. The court ruled that neither 17(a)(3) nor 15(c) concern jurisdiction and they cannot create a basis for standing where it otherwise would not exist. Moreover, because SRS invoked jurisdiction based on a federal question, the court found that SRS' failure to establish constitutional standing necessarily meant that the court lacked jurisdiction to entertain not only SRS's federal securities claims, but also its pendant state law claims. As such, the court dismissed the complaint *in toto*.

The decision is significant because it deals with an increasingly common question in litigation that arises out of mergers: namely, what must a stockholder representative do in order to secure standing to act on behalf of the former shareholders by whom it is retained? This case is, as far as we are aware, the first to address that question and the court unequivocally signaled that neither a contractual provision allowing the stockholder representative to bring the claim, the plaintiff's status as an attorney-in-fact, nor a post-filing assignment is sufficient to create constitutional standing. Rather, in order to establish standing to pursue federal and state law claims in federal court, stockholder representatives like SRS must demonstrate that they personally suffered an injury-in-fact and had some financial stake in the stockholders' claims that are plead in the complaint at the time the complaint is filed. Q

quinn emanuel
865 South Figueroa Street, 10th Floor, Los Angeles, California 90017

PRESORTED
STANDARD
U.S. POSTAGE
PAID
PERMIT NO. 4338
INDUSTRY, CA

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 David Henri at 213-443-3000.

- We are a business litigation firm of more than 650 lawyers — the largest in the world devoted solely to business litigation and arbitration.
- As of December 2013, we have tried over 2247 cases, winning 88.5% of them.
- When we represent defendants, our trial experience gets us better settlements or defense verdicts.
- When representing plaintiffs, our lawyers have garnered over $27 billion in judgments and settlements.
- We have won four 9-figure jury verdicts.
- We have also obtained thirteen 9-figure settlements and seven 10-figure settlements.

Prior results do not guarantee a similar outcome.

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

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

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

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

CHICAGO
500 West Madison St., Suite 2450
Chicago, IL 60661
312-705-7400

WASHINGTON, D.C.
777 6th Street NW, 11th Floor
Washington, DC 20001-3706
202-538-8000

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 (0) 20 7653 2000

MANNHEIM
Mollstraße 42
68165 Mannheim
Germany
+49 (0) 621 43298 6000

HAMBURG
An der Alster 3
20099 Hamburg
Germany
+49 (0) 40 89728 7000

MUNICH
Oberanger 28,
80331 Munich,
Germany
+49 (0) 89 20608 3000

PARIS
25 rue Balzac
75008 Paris
France
+33 (0)1 53 53 68 97

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 25, RBS Tower
88 Phillip Street
Sydney NSW 2000,
Australia
+61 2 8211 0690

©2013 Quinn Emanuel Urquhart & Sullivan, LLP | To update information or unsubscribe, please email updates@quinnemanuel.com.