ISRAEL PRACTICE NEWSLETTER

VOLUME 1 | ISSUE 2 | FALL 2015

Jonathan Nesher, Editor

INSIDE THIS ISSUE

Mark Kass

Q&A With Seasoned Israel-U.S. Transactional Attorney Mark Kass

We are pleased to announce that Mark Kass has joined Crowell & Moring as senior counsel in our Corporate Group and Israel Practice. Mark focuses on corporate finance, M&A, and commercial transactions, including IP license agreements and strategic agreements. His clients, who span the globe, operate in the technology and life sciences spaces, such as software, information technology, new media, telecommunications, biotech, medical devices, and cleantech.

Continued on Page 2

UPCOMING EVENTS

Nov. 11 | Washington, DC | mHealth

C&M will host a two-part program which brings together more than a dozen Israeli companies with US legal experts and introduces the Israeli companies to the broader health care community and DC area executives doing business with Israeli companies.

Nov. 16 | Tel Aviv | The US Legal Landscape in Cybersecurity, Data Protection, and Privacy: Understanding the Law, Implementing Policies, and Responding to Crises

This seminar is sponsored by Crowell & Moring and The Association of Corporate Counsel (ACC) Israel.

Nov. 17 | Tel Aviv | U.S. Cybersecurity and Homeland Security: Market Opportunities and the Legal Landscape

This seminar is sponsored by Crowell & Moring, the Fairfax County Virginia Economic Development Authority and Israel Advanced Technology Industries (IATI).

Nov. 18 | Tel Aviv | Cybersecurity Leadership Dinner

C&M hosts a program featuring Israeli and global leaders in cybersecurity.

For more information, contact Sam Feigin at sfeign@crowell.com.

Q: You have worked for over twenty years with emerging technology companies in the U.S. and in Israel, how would you compare Israeli companies with their American counterparts?

A: There are many similarities, particularly as markets become more international, and companies in the U.S. and Israel often seek to solve similar problems. But one difference comes to mind – how Israeli companies organize themselves to conduct their business.

Israeli companies are born international. From the outset, founders look outside Israel for product ideas, markets for products, capital and employees. Israeli entrepreneurs move fast to rapidly build lean local and international organizations. This business model is unusual and, when executed successfully, creates significant advantages – Israeli companies can be close to several international markets, suppliers and manufacturers, and can find talent and capital throughout the world.

Q: What are some of the challenges posed by this Israeli approach to business?

A: This business model requires nimble management. It necessitates quick judgments about partners and people around the world. These companies need to establish processes and policies across different cultures and legal systems. This is one reason why Israeli companies need an international business and legal strategy from the outset.

Q: How does your practice interact with Israeli business?

A: Twenty years ago, my wife, our children, and I moved to Israel, where we lived for four years (and where our youngest child was born), and I practiced law at a leading Tel Aviv firm. Since then, I have worked with many Israeli entrepreneurs and companies to help them build international businesses.

Much of what my colleagues and I do for Israeli companies is traditional legal work – contracts for investments or employment, commercial deals, mergers and acquisitions, U.S. regulatory matters, and helping clients navigate the US legal and regulatory systems.

Given the distance between Israeli clients and the U.S. market, I am often asked to take a more strategic, business-oriented role. My colleagues and I help clients understand the business environment in the U.S., and, sometimes serve as a client's eyes in the U.S., helping to identify potential investors, bankers, executives, consultants, and strategic partners.

At Crowell & Moring, we have tremendous legal resources and a wealth of practical experience. We have creative and accomplished lawyers in many areas of importance to Israeli companies, such as intellectual property, transactions, cybersecurity and privacy, healthcare regulation, government contracts and employment. I am very excited to have joined Crowell & Moring.

Q: In the mergers and acquisition space, what do you see on the horizon?

A: The first half of 2015 saw the highest valuations ever, with the average world-wide deal value reported to be 16 times EBIDTA, exceeding the 2007 record of 14.3x, and with reported deal sizes in Israel the highest ever. From the perspective of potential targets in Israel (and elsewhere), high valuations are good news, but we should be aware that an environment of high valuations can make it harder for parties to strike deals and we should be sensitive about the potential for a market shift downward, as was the case after the record valuations in 2007. The good news is that stock market shocks late this summer emanating from China have not seemed to derail the M&A markets in the U.S. or Israel, many potential acquirers still have large amounts of cash on hand, and interest rates remain low. It looks like large global firms continue to have a substantial appetite to acquire technology in "middle market" M&A, and Israeli companies are right in that sweet spot.

Q: What is the pressing emerging legal issue facing Israeli companies doing business in the U.S.?

A: Understanding and complying with the emerging rules relating to data privacy and cyber security, across nearly all industries. For example, U.S. private companies and the U.S. government increasingly require their suppliers and business partners to comply with standards of data privacy and cyber security, and these standards may exceed legal requirements. If data are stored on, or operations are run though, servers outside the U.S., which can be the case with Israeli companies, the laws and rules are even more complex.

Q: What are some of the changes in Israeli tech business that you have seen over the past twenty years, and what stands out for you personally over these years?

A: Perhaps not surprisingly, there are many more serial founders. I also see a greater focus on customer-centric product development. And over the years, many more businesspeople (and there are more women today) have lived in the U.S. and have a greater understanding of American business and consumer culture.

I really enjoy that I am treated as a team member, working together with management and lawyers in Israel. And I have had the chance to work with and get to know, and help, many amazing entrepreneurs and teams.

Data Protection: Safe Harbor News: Switzerland Axes It, Israel Stops Recognizing It, and U.S. Congress Acts to Save It

By Jeff Poston & Jeane Thomas

Switzerland Declares U.S.-Swiss Safe Harbor "No Longer Sufficient"

In a press release published on its website October 22, the Swiss Data Protection and Information Commissioner (FDPIC) declared the U.S.-Swiss Safe Harbor to be "no longer sufficient" for data transfers to the U.S. In essence, the FDPIC agreed with the European Union (EU) Court of Justice's (ECJ) Safe Harbor decision of October 6, even though Switzerland is not part of the European Union or governed by its courts. Over 4,400 companies had relied on the U.S.-EU Safe Harbor and over 3,400 companies had relied on the U.S.-Swiss Safe Harbor. The U.S.-EU and U.S.-Swiss Safe Harbors were nearly identical but legally distinct vehicles for data transfers.

In reference to the provisory approach of the EU Article 29 Working Party ("WP 29") for EU-U.S. data transfers, the FDPIC also recommended that companies "in the meantime" rely on "contractual guarantees" within the meaning of Article 6 para 2 lit. a of the Swiss Data Protection Act. According to the authority, this approach would not solve the issue of "disproportionate interferences," however it would temporarily improve the level of data protection.

In particular, contractual guarantees should contain the following provisions:

- Data subjects whose data is transferred to the U.S. should be informed as clearly and exhaustively as possible about the possible access to their data by the authorities, so that they can exercise their rights.
- Companies must commit to offer to affected data subjects effective legal protection to carry out the required procedures and to accept decisions on the basis of such procedures.

In line with the grace period provided by WP 29 for EU-U.S. transfers, the FDPIC now expects companies to make concerted undertakings to make the necessary adjustments to data transfers by the end of January 2016. In coordination with the European authorities, the FDPIC will examine whether further measures are necessary to guarantee that the fundamental rights of data subjects are respected. The FDPIC stated that it would be looking to "Safe Harbor 2.0" for solutions to the issues raised by the ECJ.

The statement can be found on the website of the FDPIC in French, German and Italian.

Israel's Data Protection Authority Disclaims U.S.-EU Safe Harbor

On October 20, the Israeli Law, Information and Technology Authority (ILITA) revoked its authorization to allow U.S. companies to use Safe Harbor as a way to meet onward transfer requirements under Israeli data protection law. The press release stated that companies are now required to assess whether they can use a different derogation, leaving companies to the same devices which are presumptively available in EU-U.S. data flows.

Though the U.S.-EU Safe Harbor was an agreement between the U.S. and EU, the ILITA had in practice recognized Safe Harbor-certified companies as providing "adequate" data protection with regard to transfers from Israel to the U.S. Israel, which enjoys its own "adequacy" finding from the EU, must ensure that transfers to third countries (beyond Europe and Israel) are provided "adequate" protection.

U.S. House Passes Judicial Redress Act

One lynchpin deficiency noted by the ECJ in its Safe Harbor opinion was the lack of judicial redress in the U.S. for European

citizens whose data allegedly have been collected or misused by the U.S. government. The Judicial Redress Act of 2015 is aimed to correct that by providing just such redress, not just to bolster the U.S.-EU "Safe Harbor 2.0", but to complete a key promise in the Umbrella Agreement (established for U.S.-EU law enforcement data sharing). The bill passed the U.S. House of Representatives on October 20 and now moves to the Senate, where a timeline for introduction to the floor is unknown, though many commentators are optimistic about its passage.

Jeffrey Poston

Jeane Thomas

***Jeffrey Poston** is co-chair of the firm's Privacy & Cybersecurity Group. **Jeane Thomas** is chair of the firm's E-Discovery & Information Management Group.*

Cyber/U.S. Government:

The Department of Defense's Interim Rule Emphasizes The Need for Enhanced Cybersecurity Protections

By Evan Wolff

On August 26, 2015, in a development that could be of major importance to Israeli companies doing business with the U.S. Government, the Department of Defense (DoD) published an Interim Rule that, if finalized as drafted, would expand the already onerous requirements of the Defense Federal Acquisition Regulation Supplement (DFARS) Safeguarding Clause to a broader array of potentially 10,000 defense contractors. Citing "recent high-profile breaches of federal information," the DOD's Interim Rule emphasizes the need for clear, effective, and consistent cybersecurity protections in its contracts. The Interim Rule proposes to significantly expand the scope of covered information and to require subcontractors to report cyber incidents directly to the DoD (in addition to prime contractors). Together, these changes will likely increase the scope of potential liability for government contractors and subcontractors who fail to implement adequate cybersecurity measures.

The Interim Rule seeks to enhance cybersecurity protections primarily by expanding the application of the DFARS Safeguarding Clause, which was once itself a heated point of debate. Currently, the DFARS Safeguarding Clause imposes two sets of requirements on covered defense contractors. First, they must implement "adequate security" on certain information systems, typically by implementing dozens of specified security controls. Second, they must report various cyber incidents to the DoD within 72 hours of their discovery. These requirements, however, apply only to information systems housing "unclassified controlled technical information" (UCTI), which is generally defined as controlled technical or scientific information that has a military or space application.

The Interim Rule would expand that application to information systems that possess, store, or transmit "covered defense information" (CDI). CDI would encompass UCTI, meaning that most contractors subject to the DFARS Safeguarding Clause would remain subject to the Interim Rule. But CDI goes beyond the DFARS Safeguarding Clause by also including information critical to operational security, export controlled information, and "any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government policies." Significantly, the Interim Rule lists "privacy" and "proprietary business information" as examples of the latter, leaving many covered contractors to wonder exactly how far the definition of "covered defense information" goes. To keep up with its new application, the Interim Rule would change the name of Clause 252.204-7012 from "Safeguarding Unclassified Controlled Technical Information" to "Safeguarding Covered Defense Information and Cyber Incident Reporting."

Another notable point of expansion would affect subcontractors. Under the current DFARS Safeguarding Clause, subcontractors suffering a cyber incident must report to the pertinent prime contractor, who then submits the required report to the DoD. Subcontractors do *not* report directly to the DoD under the current rule. The Interim Rule would continue to require subcontractors to report cyber incidents to their primes, but it would also require subs to

submit the required report directly to the DoD, creating the potential for inconsistent reports from the prime and sub regarding the same cyber incident.

Other key provisions of the DFARS Safeguarding Clause, however, would remain same. For example, the Interim Rule would continue to apply to all solicitations and contracts, including those for commercial items. The government would also remain required to protect any proprietary information that contractor reports pursuant to the Interim Rule. The reporting timeline of 72 hours would also remain the same, which the Interim Rule dubs "rapid reporting." Additionally, and importantly, the Interim Rule would continue to recognize the probability that even information systems with "adequate security" may still suffer a cyber incident. That is, the Interim Rule would explicitly state that the fact that a contractor has suffered a cyber incident and submitted a corresponding report would not necessarily mean that the contractor had failed to comply with the Clause's broader cybersecurity requirements.

The Interim Rule likely does not come as a surprise to many. Congress passed provisions to the National Defense Authorization Acts of 2013 and 2015 that called for the regulations that the Interim Rule now seeks to implement. The Interim Rule has thus been a long time coming, but that the DoD chose to publish it now seems appropriate. The executive branch has been implementing a whirlwind of cyber regulations specific to federal contractors, all in an effort to stem the nation's cyber vulnerabilities. Just last week, the Office of Management & Budget released proposed cybersecurity guidance that could lead to further amendments to the Federal Acquisition Regulation (FAR).

Public comments on the Interim Rule, were due on October 26, 2015.

Evan Wolff

***Evan Wollf** is co-chair of the firm's Privacy and Cybersecurity Group, and former adviser to the senior leadership at the Department of Homeland Security (DHS).*

Cyber: Is Your Company Prepared for a Cyber-Incident?

By Evan Wolff

Data security breaches are on the rise. Increasingly, companies see cybersecurity as a critical concern for their reputation and business. The stakes could not be higher. Fighting cybercrime, keeping data and proprietary information secure, and protecting networks has become a board responsibility and essential function. Success requires cooperation and management throughout the enterprise—lawyers, IT professionals, managers, security officials, communications professionals, and others need a strategy and plan.

In this three-part video alert series, Evan Wolff, Crowell & Moring partner and former Department of Homeland Security adviser, discusses the trends he's seeing in cybersecurity, how companies should prepare for cybersecurity breaches or incidents, and what companies should do when a cyber-incident or breach occurs.

Part 1: When Cybersecurity becomes a Legal Consideration

Part 2: Trends in Cybersecurity

Part 3: Preparing for Cybersecurity Breaches and Cyber Incidents

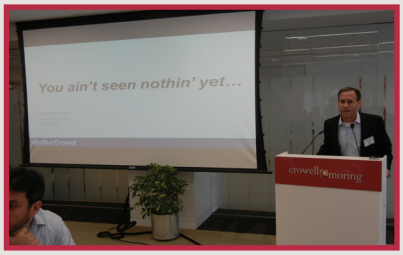
Visit our website to watch Evan's video discussions.
https://www.crowell.com/NewsEvents/AlertsNewsletters/all/VIDEO-Is-Your-Company-Prepared-for-a-Cyber-Incident

Crowell & Moring Speaks

Implications of JOBS Act & Amended SEC Rules on Emerging Companies and Raising Capital; OurCrowd Investors and C&M Focus on Tech Trends and Opportunitites

C&M Corporate Partner Kelly Howard

On **July 9, 2015** Crowell & Moring was pleased to host **OurCrowd**, and its Founder and CEO, **Jon Medved**, for a presentation and discussion with **Washington, D.C.** area entrepreneurs, executives and investors. Crowell & Moring Corporate & Securities Partner **Kelly Howard** presented on the (JOBS Act) and recently amended SEC rules that have created a number of more effective ways for early stage companies to raise capital with less effort and cost, and than a traditional IPO.

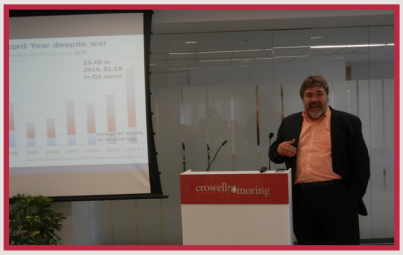


C&M's Sam Feigin, Israel Practice Chair

Sam Feigin and Mr. Medved talked about recent trends in the Israel-US tech sector and OurCrowd's impact on the ecosystem.

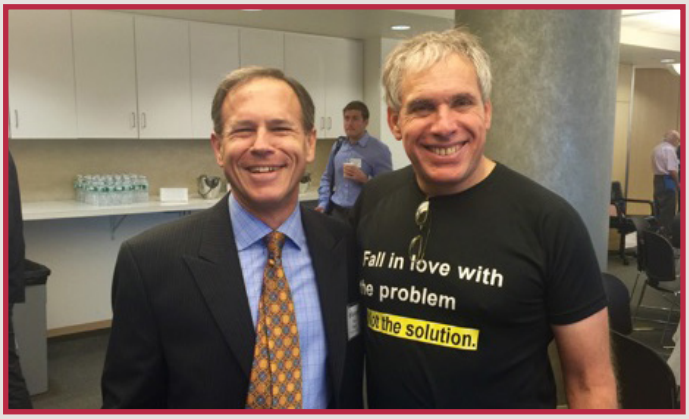
Through OurCrowd, investors are able to access investments in early stage companies with a variety of cutting edge technologies. and invest efficiently in selected companies from the perspectives of the investors and the companies.

As Mr. Medved explained, like other popular crowdfunding arrangements (such as Kickstarter), OurCrowd greatly reduces barriers to entry between interested investors and target investment opportunities. However, unlike most current crowdfunding sites that simply provide a platform for individuals or entities to solicit financial support but do not filter investors or targets, OurCrowd deploys a team of experienced investment professionals to identify, diligence and support targets in Israel, the U.S. and worldwide. Once vetted, OurCrowd negotiates offering terms based on the needs of the entity and OurCrowd's review process. Accredited investors are able to review opportunities and choose whether to invest alongside OurCrowd management and its mentor network ona company by company basis. 13, 2015. Terry presented in the context of a Fireside Chat on "How Trends in the USPTO May Impact Your Business."

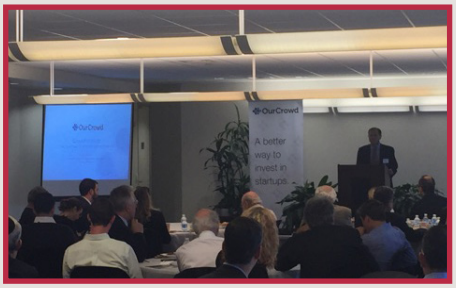


Jon Medved, longtime leader of the Israel-U.S. emerging company/venture scene

Hot Issues in M&A Deals; Uri Levine Presents on Entreprenurship and His New Portfolio Companies



C&M's Sam Feigin and Uri Levine, co-founder of Waze



Attendees at the Oct. 22 event in NY

On **October 22, 2015** Crowell & Moring hosted two investor programs in our **New York City** office in conjunction with **OurCrowd,** one for members of the high tech community and one for accredited investors. The programs featured **Uri Levine**, co-founder of Waze (acquired by Google) who has since co-founded and/or served as a director of Engie, FairFly, Fairsale, Feex, Movit, Roomer and Zeek. The program also featured Crowell & Moring's **Sam Feigin** and **Brian Blitz**, who discussed recent trends in the Israel-U.S. market and key legal issues in M&A transactions.

M&A: Representations and Warranties Insurance Key in Government Contractor M&A

By Peter Eyre & Karen Hermann

Buyers in mergers and acquisitions are usually at an informational disadvantage vis-a-vis the seller. And even with comprehensive due diligence, the buyer may still lack a full understanding of the risks and liabilities that it will inherit through the transaction. This is especially true of mergers and acquisitions involving defense and government contractors, which operate within a complex regulatory environment.

Recognizing the information asymmetry, transaction documents typically include a set of representations and warranties accompanied by indemnification provisions that allocate post-closing risk to the seller for breaches or inaccuracies in those representations or warranties. The importance of indemnification issues to both parties to the transaction means that these issues can often become deal breakers during negotiations.

Together, the parties must agree on, among other things:

- The overall scope of the seller's representations and warranties, including the allocation of known and unknown risks;
- The dollar limit of the seller's indemnity;
- The time period within which the buyer must bring its claims for breaches of the representations and warranties (the "survival period");
- The amount of escrow (if any); and
- The threshold of buyer losses, if any, triggering the seller's liability.

When parties would otherwise come to a standstill over indemnification issues, transaction risk insurance, commonly referred to as representations and warranties insurance, may bridge the gap.

The Basics of Representations and Warranties Insurance (R&W Insurance)

R&W insurance facilitates mergers and acquisitions by providing a vehicle through which the buyer and seller may reach an agreement on indemnity terms for breaches of representations and warranties. For example, the buyer may want a higher limit on the seller's potential indemnity and a longer survival period, while the seller may want to limit its liability post-closing so it can freely distribute the sale proceeds to its investors. In such a case, R&W insurance could provide the buyer with the coverage that it seeks, while allowing the seller to limit its post-closing liability to give it the freedom to distribute the sale proceeds. R&W insurance protects against unknown and unforeseen losses by offering coverage for losses that result from a seller's (or target company's) breach of the representations and warranties in the transaction documents.

Specifically, an R&W insurance policy typically covers "losses" from "claims" brought by the buyer for a breach of or alleged inaccuracy in any of the representations and warranties made by the seller. Policies usually provide blanket coverage for all representations and warranties, subject to some basic exclusions. R&W insurance can also be written to cover only specific representations and warranties, and in some cases, contingent risk insurance can be obtained to cover specific risks identified by the buyer.

R&W insurance policies are not a "cure-all." R&W insurance policies contain exclusions for purchase price adjustments, and known issues, including those discovered by the buyer during the diligence process, set out by the seller in the disclosure schedules or known by certain members of the buyer's "deal team." R&W insurance policies also frequently exclude claims for fraud, consequential damages, fines/penalties and claims for injunctive/nonmonetary relief. In addition to the more standard exclusions, R&W Insurance policies may also include deal-specific exclusions that depend on the particular representations and warranties in the transaction documents, including subject matters where the underwriter determines the buyer did not complete adequate due diligence or that the risk is generally uninsurable.

R&W insurance policies are either structured as "buyer-side" or "seller-side" policies. Buyer-side policies are first-party policies, meaning that when the buyer discovers a breach of or inaccuracy in a representation or warranty, the buyer brings its claim directly to the insurance carrier. In a buyer-side policy, the seller need not be involved in the claims process.

Seller-side policies, on the other hand, are third-party policies, meaning that the seller first receives a notice from the buyer alleging a breach of or inaccuracy in a representation or warranty and then the seller tenders the claim to the insurance

carrier. Under a seller-side policy, the seller may remain obligated to pay to defend the buyer's claim but the seller can typically receive an advancement of these costs from the insurance carrier.

Through R&W insurance, it is possible for a buyer to obtain more favorable representations and warranties than it otherwise would because the policy may have a longer survival period and a higher claim limitation than the sellers would have been willing to agree to in the transaction documents. A buyer can also use R&W insurance to enhance its bid — by enabling the buyer to offer, for example, little to no seller escrow — and thereby increasing the likelihood that the buyer's bid wins a competitive auction process.

R&W Insurance and Government Contracts Considerations

Mergers and acquisitions that involve government contractors require specialized due diligence. Given compressed deal timelines and other practical concerns (such as the inability of a buyer to conduct even rudimentary diligence on classified contracts), a buyer may not have the ability to accurately identify and cabin all of the potential risks.

There are also other issues specific to government contractors where the costs incurred, time involved and disruption caused by thorough diligence make such efforts impractical. For example, when it comes to certain intellectual property issues, deliverables must be marked accordingly or such rights can be waived. Thus, there are serious practical challenges to diligence.

In a similar vein, the counterfeit parts rule requires government contractors to pay close attention to supply chain matters. To verify this, a potential buyer might need to access lower-level employees at the target entity who may not have been read into an otherwise confidential transaction and to whom the buyer may not have easy access during the diligence process. Due to the impracticability of more fulsome diligence, buyers typically collect information on the target's policies and procedures and diligence a sampling of the target's transactions. But this might be insufficient to validate compliance in every respect.

As a result of the uncertainties in the diligence process and the considerations unique to government contracting, M&A transactions involving government contractors commonly require a robust set of representations and warranties. For example, the transaction documents will often include representations and warranties that apply to, among other things:

- All of the target's contracts, including any classified contracts;
- The risk of suspension and debarment and contract termination related to the target's present and past compliance with specific laws, rules and regulations; and
- The risk of termination or exclusion from future government contracting related to the target's compliance with socioeconomic requirements.

The nature of these representations and warranties make them all the more important to the parties and all the more likely to become deal breakers during the negotiations. Thus, R&W insurance can play a particularly important role in bridging the gap between buyer and seller in mergers and acquisitions that involve government contractors.

Conclusion

R&W insurance can help to facilitate all types of M&A transactions. But in government contracts M&A transactions, even the most comprehensive due diligence might not enable the buyer to ascertain the scope of nature of all risks, and the transaction documents must include robust representations and warranties to address these uncertainties and other considerations unique to government contractors. As a result, R&W insurance may be particularly useful when the M&A transaction involves government contractors and may even make the difference between a closed transaction and a busted deal.

Originally published by Law360 on September 3, 2015.

Peter Eyre

Karen Hermann

***Peter Eyre** is a partner in the firm's Government Contracts Group. **Karen Hermann** is a partner in the firm's Corporate Group.*

IP: Tech Companies and Inventors and the Emerging U.S. Patent and Trademark Office (PTO) Trend: Patent Trial and Appeal Board (PTAB) Decisions Suggest That Petitioner's Motive is Irrelevant When Instituting *Inter Partes* Review Petitions

By Brian Koide

The new PTAB trial proceedings in the PTO offer a new avenue for companies that may be charged with infringing a patent. Third parties can request *inter partes* review of another party's patent. The cost and time savings are considereable when compared to litigating in a District Court. Surprisingly these proceedings before the PTAB are being used by entities who will never be charged with infringement. This area of the law is just being sorted out and is discussed below.

In particular, does a petitioner's motive in filing an *Inter partes* review (IPR) petition matter when deciding whether to institute such proceedings? Based on two of its recent decisions, the Patent Trial and Appeal Board (PTAB) has suggested that a petitioner's motive is irrelevant as long as the underlying basis to challenge the patent has merit. Though these decisions are subject to review, in effect the PTAB rejected arguments that it is improper to institute an IPR when the petitioner's ostensible motive is merely profit-driven, as opposed to a competitive interest in invalidating a patent. This is good news for certain hedge funds and public interest organizations. A small number of hedge funds, for instance, have been filing IPR petitions and then "shorting" the patent owner's stock—a transaction that, in essence, bets on the stock price going down—or buying stock of a patent owner's competitors with the expectation that the IPR petition will either lower the price of the patent owners' stock or increase the price of its competitors. On the receiving end, it is bad news for companies whose stock price is tied closely to a single patent or small patent portfolio as they may see an uptick of IPR challenges.

IPRs are relatively new post-grant proceedings where the validity of a patent may be challenged in an administrative proceeding before the PTAB. Under the America Invents Act (AIA) statute, an IPR petition may be filed by any entity that does not own the patent at issue, and there is no requirement that the petitioner be an accused infringer, a competitor, or have any other interest tied specifically to the patent. *See* 35 U.S.C. § 311.

On September 25, 2015, in Coalition for Affordable Drugs VI, LLC v. Celgene Corp., IPR2015-01092, -01096, -01102, -01103, and -01169, the PTAB denied a sanctions motion filed by patent owner Celgene. Celgene argued that the Petitioner—a wholly-owned subsidiary of a hedge fund—abused the IPR process and that the petition should be dismissed because it was "driven entirely by an admitted 'profit motive' unrelated to the purpose of the [AIA], and unrelated to a competitive interest in the validity of the challenged patents." The PTAB rejected both arguments, stating that "[p]rofit is at the heart of nearly every patent and nearly every *inter partes* review" and noted that "an economic motive for challenging a patent claim does not itself raise abuse of process issues." The PTAB also rejected any limitation on IPRs to those parties "having a specific competitive interest in the technology covered by the patents." Finally, in noting that there was no allegation that the petitions were without merit, the PTAB explained that "[t]he AIA was designed to encourage the filing of meritorious patentability challenges, by any person who is not the patent owner, in an effort to further improve patent quality."

More recently, on October 7, 2015, the PTAB decided to institute IPR in The Mangrove Partners Master Fund, Ltd. v. VirnetX Inc., IPR2015-01046. VirnetX is a publicly-traded IP company (PIPCO) that has asserted its portfolio of patents against many high-tech companies. Mangrove, a hedge fund, was apparently seeking to use the IPR to financially benefit from any decline in VirnetX's stock price. The PTAB rejected VirnetX's argument that it "'should ... refuse to institute this IPR' because '[t]his proceeding was filed in an apparent attempt to manipulate the financial markets.'" As in *Celgene*, the PTAB explained that an economic motive for requesting IPR is not by itself improper and again noted that there was no question as to the merit of Mangrove's patentability challenge.

The PTAB's decisions in *Celgene* and *VirnetX* will likely have two effects. First, on the petitioner side, we would expect to see an increased number of petitioners that face accusations or suits involving the patent they seek to invalidate. In addition to hedge funds and other investment institutions, we would anticipate certain public interest entities that wish to invalidate patents on policy grounds to file IPRs. Similarly, industry organizations (whose members may be accused of infringement or otherwise face exposure) may also turn to IPRs on behalf of

their members. Second, on the patent owner side, we would expect to see IPR challenges not only against pharmaceutical companies and PIPCOs, but also any public company with a stock value that is closely linked to a single patent or small set of patents. Such companies could further insulate themselves from such IPR attacks by diversifying their patent portfolios and product lines.

Brian Koide

Brian Koide is a partner in the firm's Intellectual Property Group.

IP: Unitary Patent and Unified Patent Court for Europe

By Kristof Roox and Jan-Diederik Lindemans

Inevitable and Fundamental Change

The launch of the Unitary Patent (UP) and the Unified Patent Court (UPC) will remodel the European patent landscape. The so-called "EU Patent Package" consists of three legislative acts: a Regulation on UP protection, a Regulation on the language regime for the UP, and an Agreement setting up the UPC. This package will inevitably and fundamentally change the way patents are granted and enforced in the EU.

How Will the New System Work?

At the request of the patent proprietor, a UP, once granted by the European Patent Office, will benefit from unitary effect in the participating member states. It is therefore a supplementary and optional instrument that multinational companies, SMEs, or individuals will have at their disposal. Patent applicants will therefore still be able to apply either for a (series of) national patent(s), or for a European patent under the European Patent Convention (to take effect in one or more of the Convention's contracting states).

The UP will not only provide EU-wide uniform protection and have equal effect in all the participating member states, it will also offer an interesting alternative vis-à-vis cost. Indeed, the cost of obtaining unitary effect will be lower than the cost of validating a European or multiple national patents in the different designated states. The new patent system will also be easier to manage: a single annual renewal fee, a single set of rules, a single jurisprudence, and a single Court. As a result, decisions on validity or infringement with effect across the whole of the territory of the participating member states will become a reality.

Unified Jurisprudence on Patent Law

The new system sets up a single court (the UPC) for litigation relating to the infringement and validity of patents. The aim of the UPC is to enhance legal certainty by creating a unified jurisprudence, providing a single forum for patent litigation, and to improve the enforcement of patents throughout Europe.

More precisely, the Agreement on the UPC creates a new specialist patents court that will be common to all the participating states. This court will have exclusive jurisdiction for litigation relating to the UP and will even in some cases have jurisdiction in respect of old style European patents, and supplementary protection certificates. A pan-European (preliminary or permanent) injunction, as well as a pan-European revocation will therefore become possible. However, the UPC will not have jurisdiction over national patents.

The UPC will consist of a Court of First Instance (comprising central, local, and regional divisions), a Court of Appeal, and a Registry. Local and regional divisions will have the competence to handle infringement actions, while the central division will be concerned with revocation matters and declarations of non-infringement. To encourage the use of alternative dispute resolution for patent disputes, the Agreement also establishes a mediation and arbitration center.

Pro-active Planning Is a Must

The above is excellent in theory, but creates some significant challenges in practice. The new system has indeed been created from scratch and draws inspiration from different legal cultures. Although the newly created rules are elaborate, they remain incomplete and on occasion even unclear. With the Rules of Procedure virtually finalized, it is clear that the management and enforcement of European patent portfolios will require pro-active planning. Given the many different angles and aspects of the UP(C) most patentees and licensees will have difficulties successfully executing their patent strategies on their own. Lawyers in our European office are uniquely positioned to help

local and international clients understand how these changes will impact their existing patent and license portfolios and advise on appropriate courses of action.

Kristof Roox

Jan-Diederik Lindemans

***Kristof Roox** and **Jan-Diederik Lindemans** are partners in the firm's Intellectual Property Group.*

FDA: Pharmaceutical Company Launches First U.S. Biosimilar

By Terry Rea & Keith Harrison

On September 3, 2015 Sandoz, a world leader in generic pharmaceuticals, launched the first U.S. biosimilar after the Federal Circuit's *Amgen v. Sandoz* decision on September 2 to deny the request by Amgen, an American multinational biopharmaceutical company, to extend the injunction that had prevented the launch.

The FDA defines a biosimilar product as, "a biological product that is approved based on a showing that it is highly similar to an FDA-approved biological product, known as a reference product, and has no clinically meaningful differences in terms of safety and effectiveness from the reference product. Only minor differences in clinically inactive components are allowable in biosimilar products."

The injunction barring launch was set to expire and Amgen moved to extend the stay while the full Federal Circuit considers Amgen's petition for *en banc* review of its July 21 ruling that would allow the launch. The motion was denied without comment, in a 2-1 split decision.

This represents the latest development in an ongoing litigation over the first biosimilar to gain approval in the U.S. Sandoz had filed an abbreviated biologics license application (aBLA) with the Federal Drug Administration (FDA). Once the application was accepted, Sandoz notified Amgen of its intention to launch once it gained approval.

Sandoz also refused to provide its aBLA and manufacturing information to Amgen by the end of the statutory deadline. On this basis, Amgen filed suit in the Northern District of California. There, the court held that (1) disclosure of a biosimilar applicant's Biologic License Application (BLA) and proprietary manufacturing information to the reference product sponsor is permissive; and (2) that a biosimilar applicant is required to give the reference sponsor 180-day notice of the first commercial marketing of the biosimilar only **after** the biosimilar is approved by the FDA.

As we previously reported, the Federal Circuit had held that Sandoz did not violate the Biologics Price Competition and Innovation Act (BPCIA) by not disclosing its aBLA and the manufacturing information by the statutory deadline.

Amgen petitioned the full Federal Circuit to revisit that interpretation of the BPCIA and moved to continue the injunction preventing Sandoz's launch pending that determination. Amgen's petition for *en banc* review is still pending.

Terry Rea

Keith Harrison

***Terry Rea** is a partner in the firm's Intellectual Property Group and is the former acting and deputy director of the United States Patent and Trademark Office (USPTO). She was a featured speaker at the 2015 IP Best Practices conference and Life Science Leadership Dinner in Tel Aviv. **Keith Harrison** is a partner in the firm's Litigation & Trial Department.*

Further Information

If you have questions or would like additional information related to the content provided in this newsletter, please contact the authors or Sam Feigin, Chair of Crowell & Moring's Israel Practice.

https://www.crowell.com/Practices/Israel-Practice

About Crowell & Moring's Israel Practice

Our Israel Practice provides one-stop strategic and legal advice to Israeli companies doing business in the U.S. and multinationals partnering with Israeli companies. We handle the complete array of issues that Israel-related businesses tend to experience, from intellectual property advice on the first idea, to corporate and employment representation in the establishment and financing of the entity, to securities work on the public offering, through M&A representation in conjunction with the sale of the company.

We understand the fast-paced, cutting-edge needs of Israeli companies, investors, executives and entrepreneurs. We anticipate issues and opportunities and operate proactively, quickly, and creatively. We are deeply ensconced in the most relevant sectors including:

- High Tech
- Technology, Media & Telecommunications
- Internet
- Cybersecurity
- Aerospace & Defense
- Pharmaceuticals & Life Sciences
- Energy/Clean Tech
- Retail & Consumer Products

We handle virtually every type of legal work needed by Israeli companies doing business in the U.S. and around the world. Areas of focus include:

- Mergers & Acquisitions
- Intellectual Property
- Formation of U.S. Entities & Tax Planning
- Financing, including venture capital and debt financings
- Public Offerings
- Government Contracts
- International Litigation & Dispute Resolution
- Labor & Employment
- Advertising & Product Risk Management
- International Trade and Customs
- Joint Ventures and Franchising
- Licensing and Strategic Collaborations

We facilitate business opportunities for our clients by early identification of market openings, private and government RFPs, technology trends, investor desires, compelling technology and the like, and by making introductions to potential business partners. Our extensive relationships with Fortune 500 companies, category killers, private equity leaders, and venture capital funds enable us to introduce Israeli emerging companies to the most sought after investors and strategic partners. And our vast network in the Israeli business community allows us to introduce our industry-leading multinational clients to compelling Israeli technologies and products, and those who create them.

Israel Practice Chair

Samuel E. Feigin
Partner
sfeigin@crowell.com
Washington, D.C.
202.624.2594

Sam Feigin is chair of C&M's Israel practice, co-chair of the Emerging Companies/Venture Practice, and a member of the Life Science Steering Committee. He is a Chambers-ranked M&A/Corporate attorney and leading Employment attorney with more than 20 years of legal experience who is also the founder of the Network for US-Israel Business.

Newsletter Editor and Israel Practice Member

Jonathan Nesher
Associate
jnesher@crowell.com
Washington, D.C.
202.624.2743

Jonathan Nesher is an attorney in the firm's Corporate Group whose practice includes representing public and private companies in transactional matters. Prior to joining C&M, Jon served as senior legal and strategic advisor in the Office of the Prime Minister of Israel. He is a graduate of Harvard Law School and the Naval Academy of the Israel Defense Forces, where he served as commander of a naval warship and earned the rank of Captain.